

УТВЕРЖДЕН

ЦАУВ.14001-02 32 01-ЛУ

**Клиентская операционная система  
с интегрированными пользовательскими приложениями  
МСВСфера 7.3 АРМ**

**Руководство администратора**

**ЦАУВ.14001-02 32 01**

Версия 1.0

Инов. № подл.	Подпись и дата	Взам. инв №	Инов. № дубл.	Подпись и дата

Изм	Лист	№ докум	Подп	Дата

## АННОТАЦИЯ

Настоящее руководство предназначено для администраторов клиентской операционной системы с интегрированными пользовательскими приложениями МСВСфера 7.3 АРМ.

Руководство ориентировано на специалистов, знакомых с операционными системами типа Linux и имеющих минимальный практический опыт работы с ними.

Руководство снабжено иллюстрирующими примерами, сделанными в операционной системе МСВСфера 7.3 АРМ, установленной в базовой конфигурации.

Изм	Лист	№ докум	Подп	Дата

## СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ</b> .....	6
<b>1 УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ</b> .....	7
1.1 Подготовительные процедуры.....	7
1.2 Системные требования.....	9
1.3 Порядок установки и настройки.....	9
<b>2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ</b> .....	18
2.1 Утилита useradd .....	18
2.2 Утилита usermod .....	20
2.3 Утилита userdel .....	21
2.4 Утилита groupadd .....	22
2.5 Утилита groupmod .....	23
2.6 Утилита groupdel.....	23
2.7 Утилита passwd.....	24
2.8 Утилита chage.....	26
2.9 Утилита id.....	27
2.10 Конфигурационный файл /etc/login.defs.....	28
2.11 Конфигурационный файл /etc/pam.d/system-auth.....	28
2.12 Конфигурационный файл /etc/issue.....	33
2.13 Конфигурационный файл /etc/shadow.....	33
<b>3 УПРАВЛЕНИЕ ДОСТУПОМ</b> .....	35
3.1 Утилита chmod .....	35
3.2 Утилита chown .....	37
3.3 Утилита chgrp .....	37
3.4 Утилита setfacl .....	38
3.5 Утилита getfacl .....	38
3.6 Утилита seinfo.....	42
3.7 Утилита setenforce .....	42
3.8 Утилита setfiles.....	42

Изм	Лист	№ докум	Подп	Дата

3.9	Утилита restorecon .....	43
3.10	Утилита chcon.....	43
3.11	Утилита edquota.....	44
3.12	Конфигурационный файл /etc/profile.....	44
3.13	Конфигурационный файл /etc/security/limits.conf.....	47
3.14	Конфигурационный файл /etc/fstab.....	49
<b>4</b>	<b>РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ.....</b>	<b>51</b>
4.1	Утилита auditctl.....	51
4.2	Утилита autrace .....	53
4.3	Утилита ausearch.....	54
4.4	Утилита aureport .....	56
4.5	Конфигурационный файл /etc/audit/audit.conf.....	58
<b>5</b>	<b>ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ.....</b>	<b>62</b>
5.1	Утилита chkconfig .....	62
5.2	Утилита systemctl .....	63
5.3	Утилита crontab .....	64
5.4	Утилита rpm .....	65
5.5	Утилита yum.....	66
<b>6</b>	<b>СТИРАНИЕ ДАННЫХ.....</b>	<b>68</b>
6.1	Утилита shred.....	68
6.2	Утилита sfill .....	68
6.3	Утилита sswap.....	69
6.4	Утилита sdmem.....	70
<b>7</b>	<b>КОНТРОЛЬ ЦЕЛОСТНОСТИ.....</b>	<b>71</b>
7.1	Утилита md5sum .....	71
7.2	Утилита aide .....	72
<b>8</b>	<b>ОБЕСПЕЧЕНИЕ НАДЕЖНОГО ФУНКЦИОНИРОВАНИЯ.....</b>	<b>74</b>
8.1	Утилита tar .....	74
8.2	Утилита cpio .....	75

Изм	Лист	№ докум	Подп	Дата

8.3	Утилиты amanda .....	76
8.4	Утилита mdadm .....	77
<b>9</b>	<b>ФИЛЬТРАЦИЯ СЕТЕВОГО ПОТОКА.....</b>	<b>80</b>
9.1	Утилита firewall-cmd.....	80
9.2	Конфигурационный файл /etc/firewalld/firewalld.conf.....	82
<b>10</b>	<b>МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ.....</b>	<b>85</b>
10.1	Утилита logwatch .....	85
10.2	Утилита top.....	85
10.3	Утилита ps.....	87
10.4	Утилита tcpdump.....	87
10.5	Утилита ac.....	88
10.6	Утилита lastcomm.....	88

Изм	Лист	№ докум	Подп	Дата

## ВВЕДЕНИЕ

МСВСфера 7.3 АРМ – клиентская операционная система на основе ядра Linux с набором интегрированных пользовательских приложений, включающим пакет офисных программ, браузер, почтовую программу, редакторы текстов и графики, проигрыватели аудио и видео, менеджеры файлов и архивов, программу записи и копирования оптических дисков, программу сканирования документов, множество других программ, а также средства администрирования и защиты информации.

МСВСфера 7.3 АРМ – удобная в использовании операционная система, предназначенная для организации многофункциональных рабочих мест на базе 64-х разрядных аппаратных платформ Intel и AMD. Как правило, она совместима со средствами вычислительной техники, выпущенными в течение последних нескольких лет. Однако, в связи с непрерывным их совершенствованием, в некоторых случаях целесообразно предварительно ознакомиться с соответствующими техническими описаниями и удостовериться в такой совместимости путем пробного тестирования.

В данном руководстве приведен перечень подготовительных процедур, направленных на обеспечение безопасности при внедрении и использовании операционной системы МСВСфера 7.3 АРМ, дано краткое описание порядка ее установки и настройки, а также описание интерфейсов основных средств администрирования и их функциональных возможностей.

Изм	Лист	№ докум	Подп	Дата

## 1 УСТАНОВКА И НАСТРОЙКА СИСТЕМЫ

### 1.1 Подготовительные процедуры

Внедрению и использованию операционной системы должны предшествовать подготовительные процедуры, направленные на обеспечение безопасности при приемке установочного дистрибутива операционной системы от поставщика, на обеспечение безопасной установки, настройки и запуска операционной системы и на создание безопасной среды ее функционирования. Реализация подготовительных процедур должна обеспечиваться необходимыми ресурсами и сопровождаться назначением ответственных за их выполнение должностных лиц.

Процедуры безопасной приемки должны предусматривать меры подтверждения подлинности установочного дистрибутива операционной системы, исключающие возможности преднамеренного или непреднамеренного внесения изменений в поставляемую версию, т.е. замены ее фальсифицированной или неработоспособной версией. К таким мерам в общем случае относятся:

проверка подлинности источника поставки путем визуального контроля наличия и целостности специальных защитных стикеров (наклеек, знаков) на упаковке комплекта поставки, а также целостности самой упаковки;

проверка комплектности поставки в соответствии с заявкой, договорными материалами и спецификацией, сверка маркировки и номера версии;

проверка целостности установочного дистрибутива с помощью программного средства контроля целостности путем сравнения с приведенным в эксплуатационной документации эталонным значением контрольной суммы или с помощью средств электронной подписи.

Процедуры безопасной установки, настройки, запуска операционной системы и создания безопасной среды ее функционирования в общем случае должны предусматривать меры, обеспечивающие:

совместимость операционной системы со средствами вычислительной техники, на которых планируется ее установка и использование;

установку, конфигурирование, настройку, запуск и управления операционной системой в соответствии с эксплуатационной документацией и принятой политикой безопасности;

Изм	Лист	№ докум	Подп	Дата

защиту от действий, направленных на нарушение физической целостности средств вычислительной техники, на которых она функционирует;

доверенную загрузку операционной системы, контроль доступа к процессу загрузки, блокирование попыток несанкционированной загрузки, контроль целостности компонентов загружаемой операционной среды;

наличие ресурсов для выполнения функциональных возможностей безопасности операционной системы, хранения создаваемых резервных копий, а также защищенное хранение данных операционной системы и защищаемой информации;

ограничение на установку программного обеспечения и его компонентов, не задействованных в технологическом процессе обработки информации.

доверенный маршрут между операционной системой и пользователями;

доверенный канал передачи данных между операционной системой и средствами вычислительной техники, на которых происходит обработка информации, а также с которых происходит их администрирование;

невозможность отключения или обхода компонентов операционной системы и средств защиты информации.

препятствие несанкционированному копированию информации, содержащейся в операционной системе, на съемные машинные носители информации, в том числе контроль вноса (выноса) в (из) контролируемую зону съемных машинных носителей информации;.

проверку целостности получаемых от поставщика внешних модулей уровня ядра перед их установкой в операционную систему;

выделение вычислительных ресурсов для процессов в соответствии с их приоритетами;

профессиональную компетентность и надежность персонала, ответственного за администрирование системы, его способность выполнять свои обязанности в точном соответствии с принятой политикой безопасности и эксплуатационной документацией;

возможность генерации аутентификационной информации, соответствующей заданной метрике качества;

недоступность аутентификационной информации для лиц, не уполномоченных на ее использование;

разделение полномочий пользователей и администраторов с назначением им минимально необходимых прав и привилегий;

Изм	Лист	№ докум	Подп	Дата



исключение в процессе использования системы доступа пользователей к приложениям, выполняющимся с более высокими правами доступа, чем права, предоставленные им согласно матрице доступа;

завершение администраторами приложений, запущенных ими с административными правами после окончания работы с ними;

запрет пользователям на передачу посторонним лицам своей личной идентификационной и аутентификационной информации, а также на регистрацию кого-либо в системе под своим именем и паролем.

## 1.2 Системные требования

Для использования операционной системы требуется компьютер со следующими минимальными характеристиками: 64-х битный процессор Intel или AMD, 1 Гб оперативной памяти, от 8-ми до 11-ти Гб свободного пространства памяти на жестком диске в зависимости от используемой конфигурации.

## 1.3 Порядок установки и настройки

Перед началом установки необходимо уточнить тип и интерфейс микропрограммной прошивки материнской платы компьютера, после чего в ее настройках соответствующим образом отключить параметр Secure Boot, переведя его из состояния Enable в состояние Disable. В некоторых редакциях прошивки необходимо также для параметра OS Type выбрать значение Other OS (Legacy OS или т.п.).

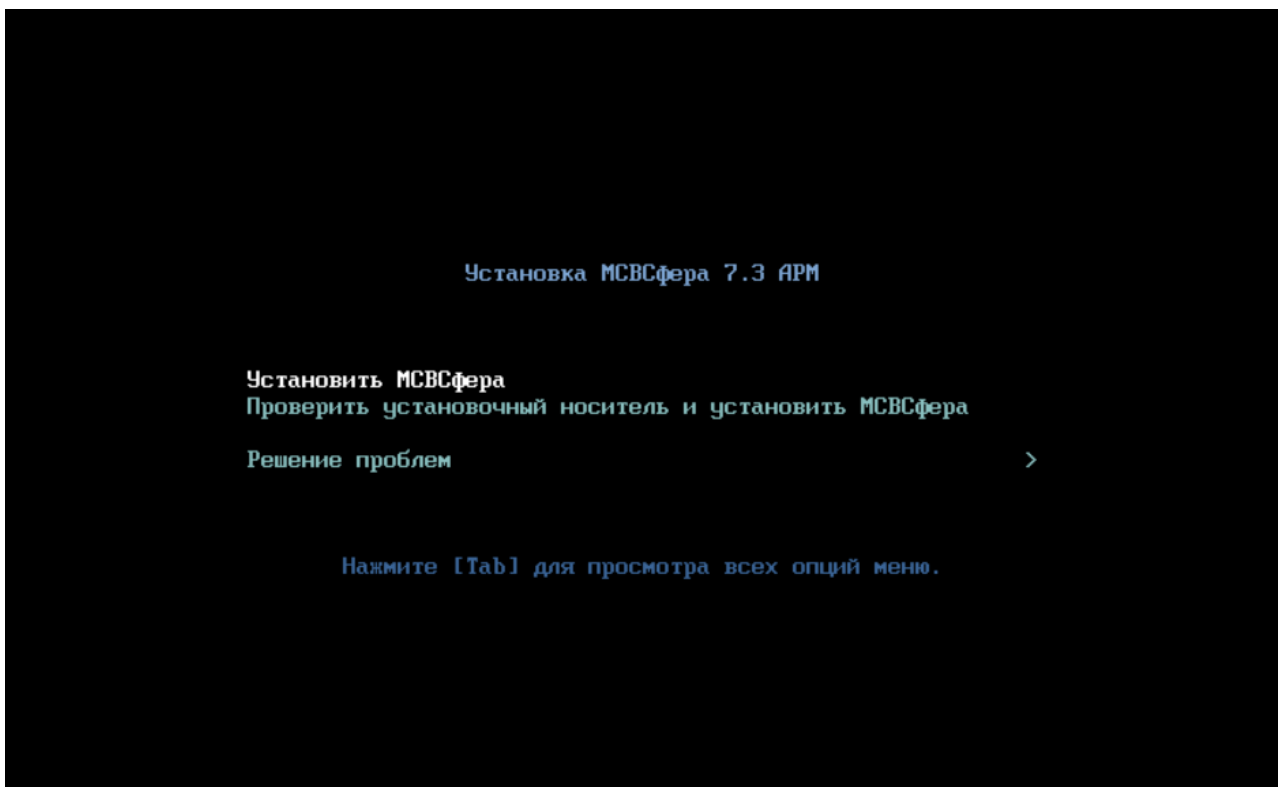
Существуют различные варианты установки. Ниже описан вариант установки с оптического диска, подразумевающий соответствующую приоритетную поддержку базовой системы ввода/вывода. Установка и настройка системы производится следующим образом.

Вставьте диск с установочным дистрибутивом в устройство чтения данных с оптических дисков и произведите запуск компьютера. Сначала установка будет проходить в текстовом режиме (см. Снимок экрана 1), потом она продолжится в графическом режиме и на экране монитора компьютера появится окно с предложением выбрать язык установки (см. Снимок экрана 2). Затем появится окно Обзор установки (см. Снимок экрана 3), с помощью которого последовательно нажимая расположенную в верхнем левом углу кнопку Готово можно будет произвести все необходимые настройки, а именно: дата и время (см. Снимок экрана 4), раскладка клавиатуры (см. Снимок экрана 5), языковая поддержка (см. Снимок

Изм	Лист	№ докум	Подп	Дата

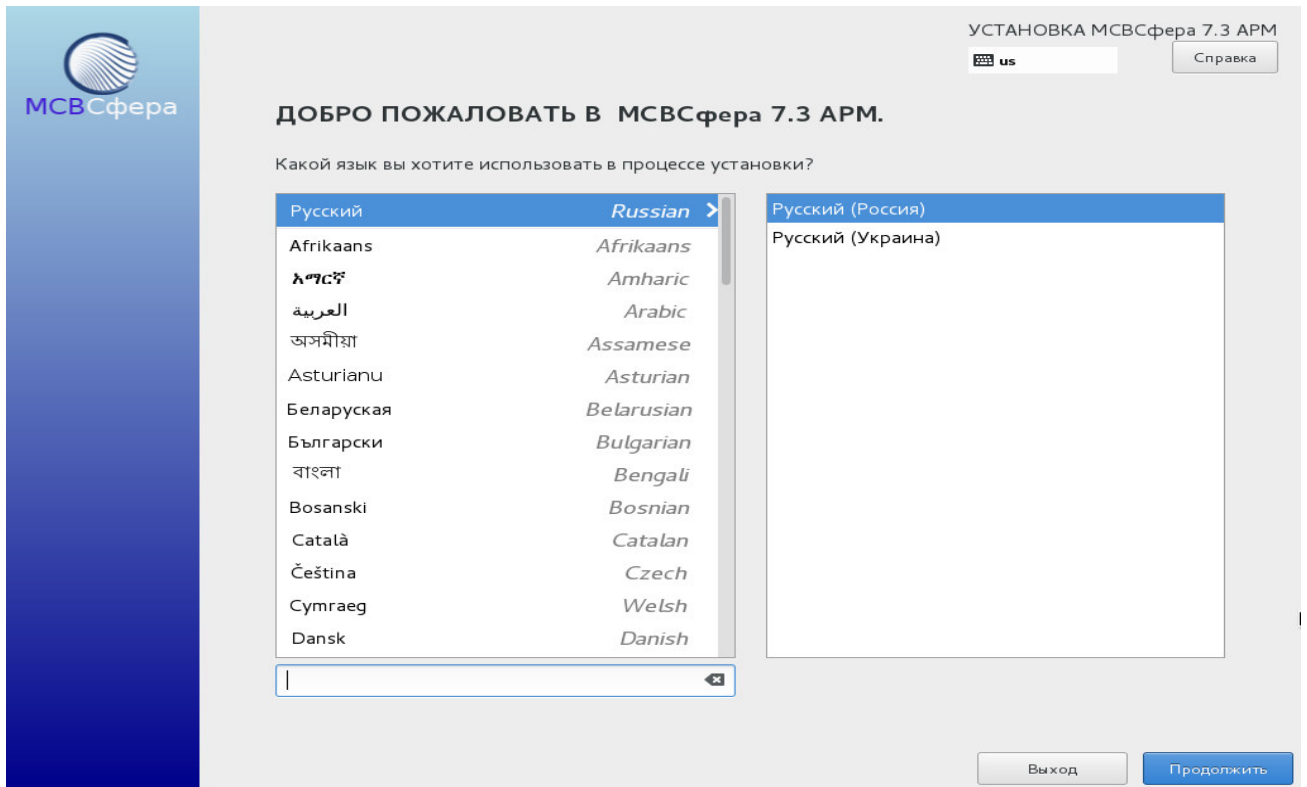
экрана 6), источник установки (см. Снимок экрана 7), выбор программ (см. Снимок экрана 8), место установки (см. Снимок экрана 9), сеть и имя узла (см. Снимок экрана 10), диагностика сбоя ядра (см. Снимок экрана 11). После того, как все необходимые настройки произведены, можно нажать нижнюю правую кнопку Начать установку (см. Снимок экрана 3) и процесс установки начнется. Его продолжительность может составить примерно до одного часа, в зависимости от быстродействия компьютера и выбранной конфигурации программного обеспечения. В процессе установки системой будет предложено задать пароль так называемого суперпользователя root (см. Снимки экрана 12, 13) и создать нового пользователя (см. Снимки экрана 14, 15). По завершении установки на экране монитора появится соответствующее уведомление с предложением произвести перезагрузку. После извлечения диска с установочным дистрибутивом и перезагрузки системы появится приглашение войти в систему, пройдя идентификацию и аутентификацию.

Следует иметь в виду, что по умолчанию беспроводная связь Bluetooth находится в отключенном состоянии. Для ее включения администратору необходимо удалить конфигурационный файл /etc/modprobe.d/disable-bluetooth.conf и перезагрузить компьютер, а для отключения необходимо вернуть данный файл на место и снова выполнить перезагрузку.

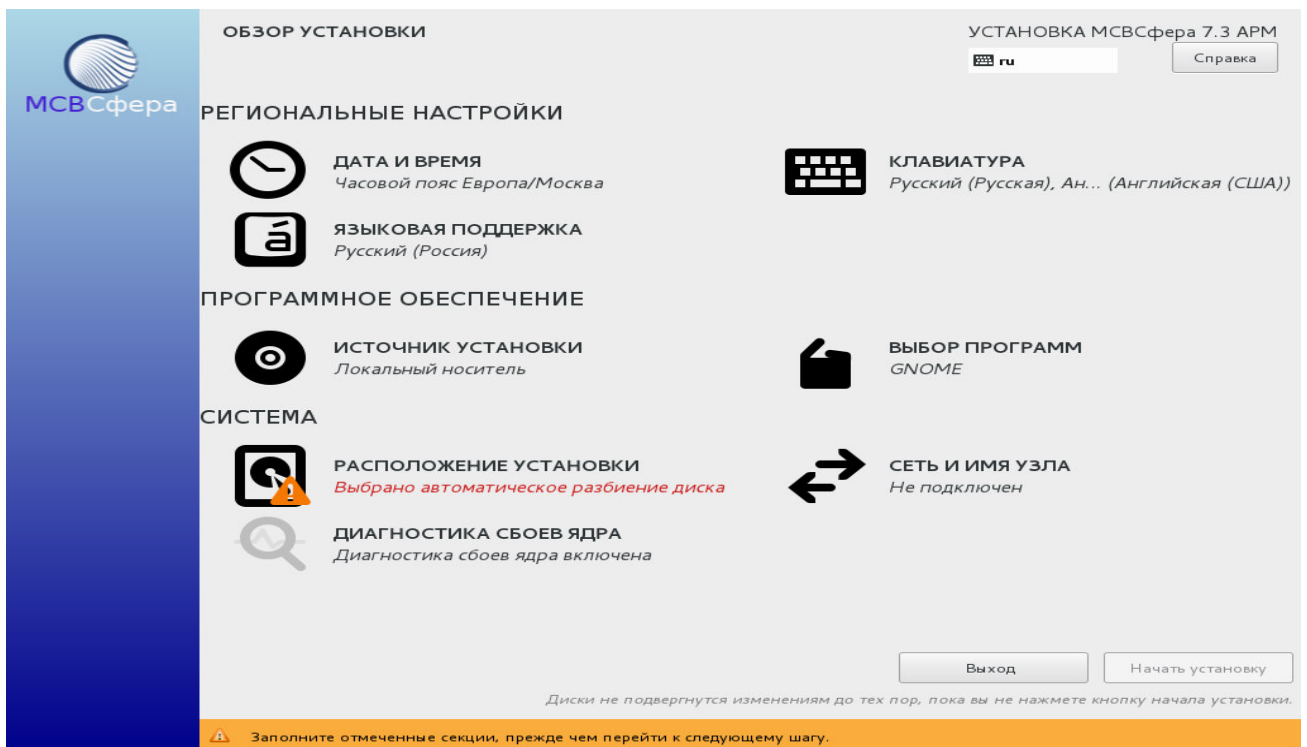


Снимок экрана 1 - Начало установки

Изм	Лист	№ докум	Подп	Дата

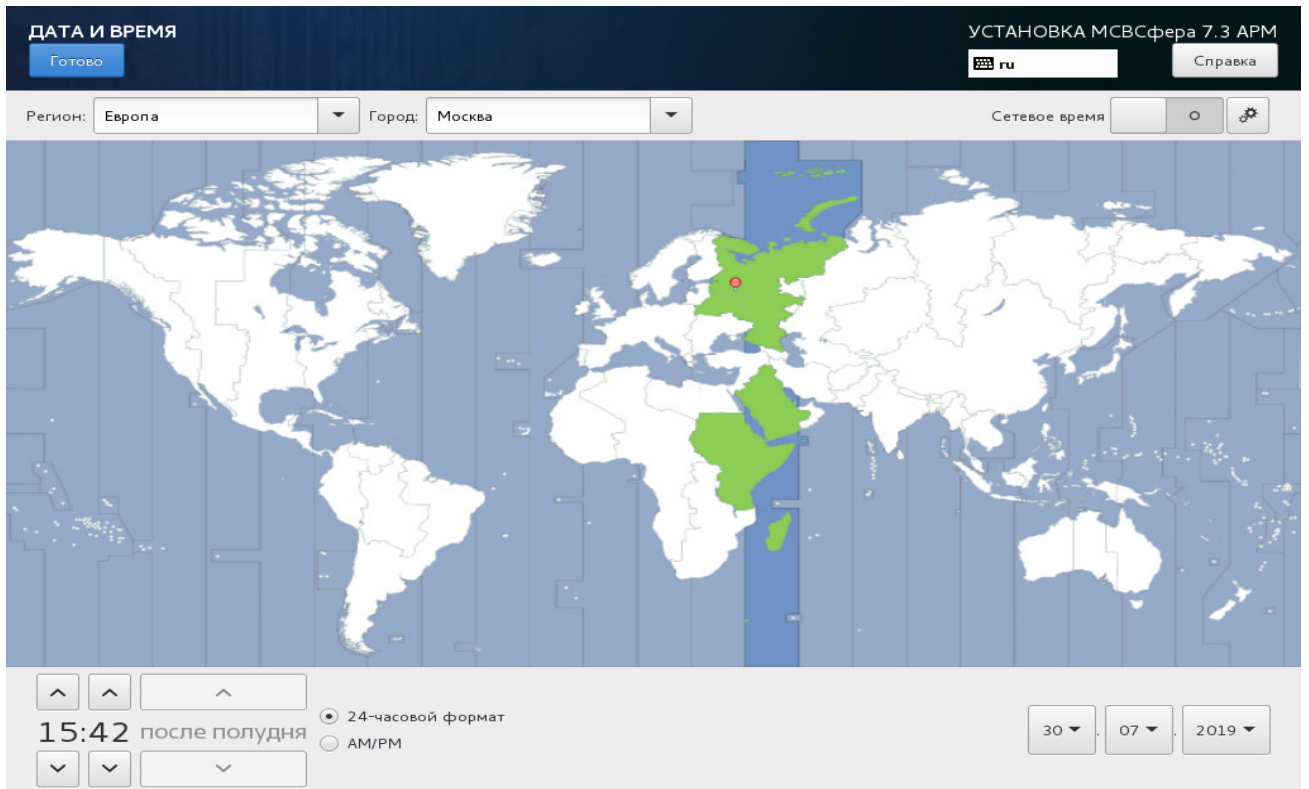


Снимок экрана 2 - Язык установки

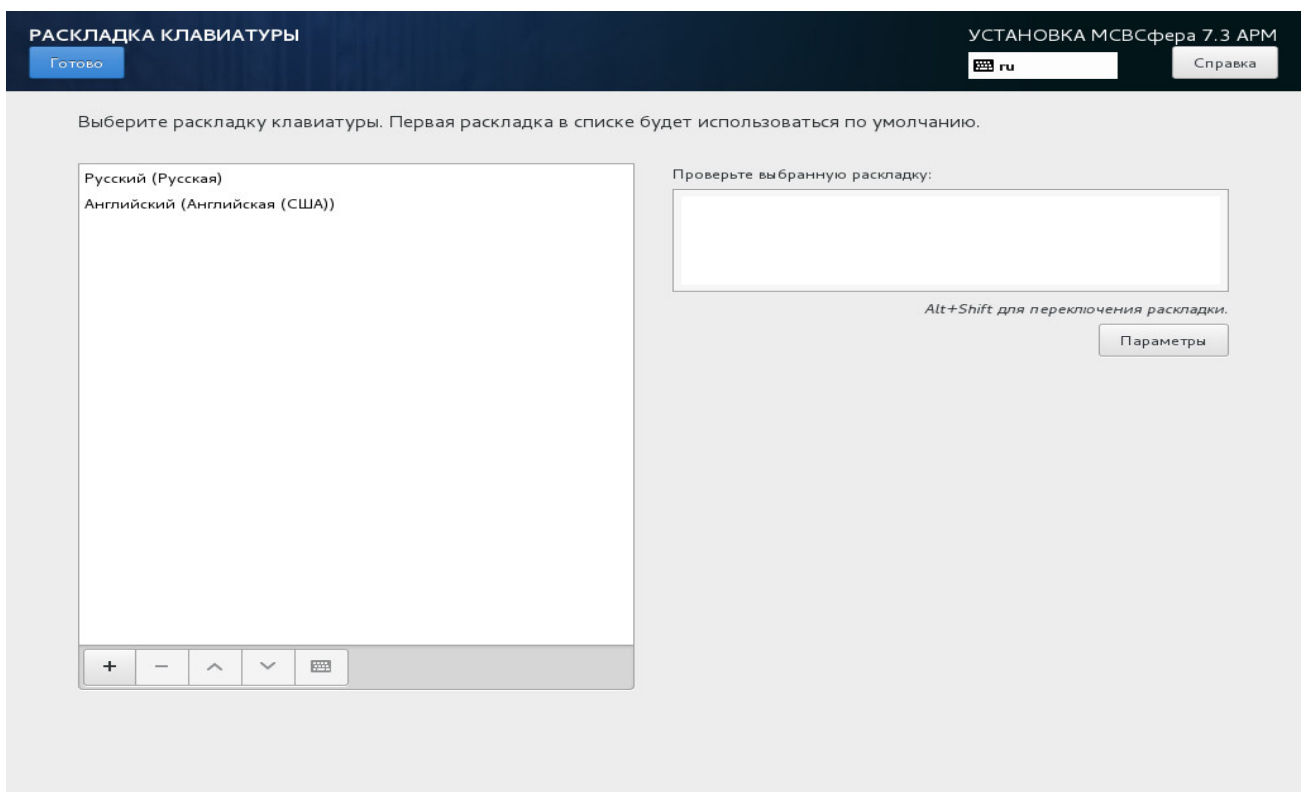


Снимок экрана 3 - Обзор установки

Изм	Лист	№ докум	Подп	Дата

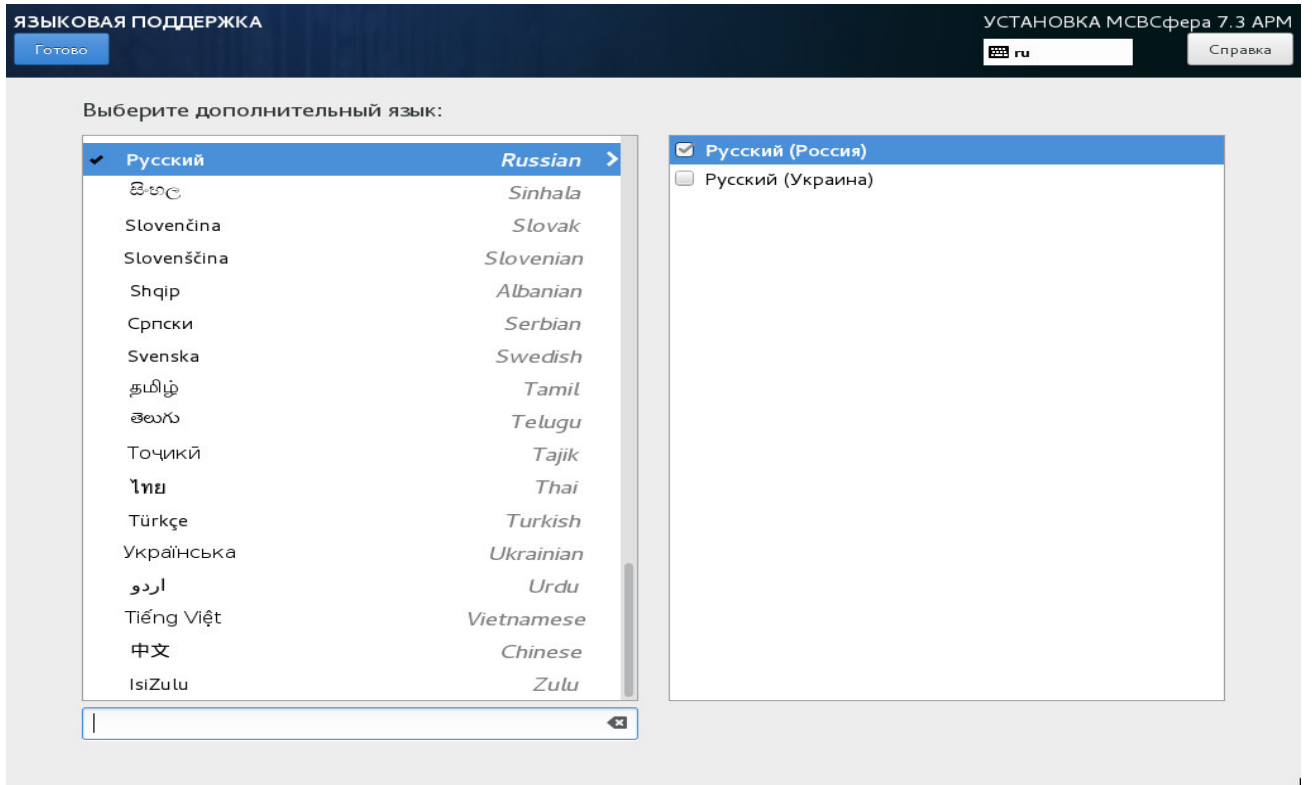


Снимок экрана 4 - Дата и время

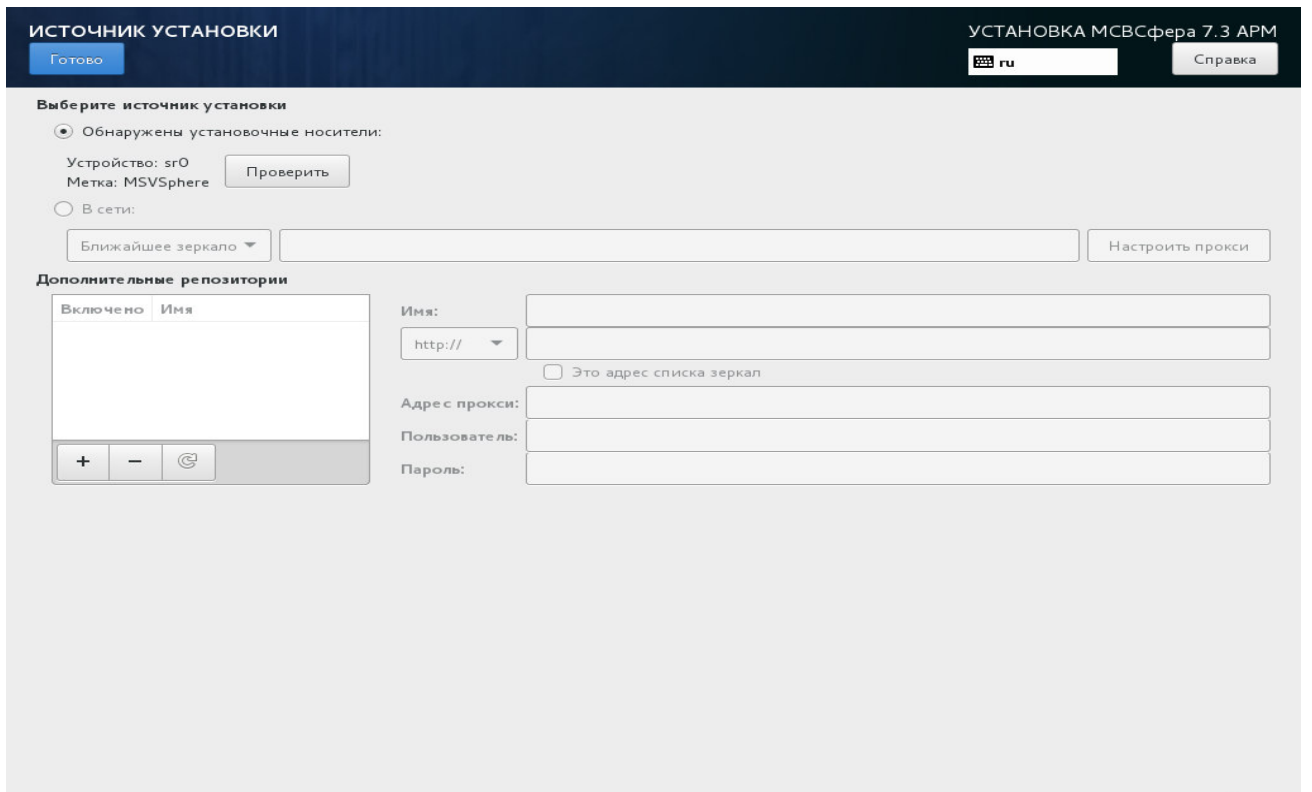


Снимок экрана 5 - Раскладка клавиатуры

Изм	Лист	№ докум	Подп	Дата

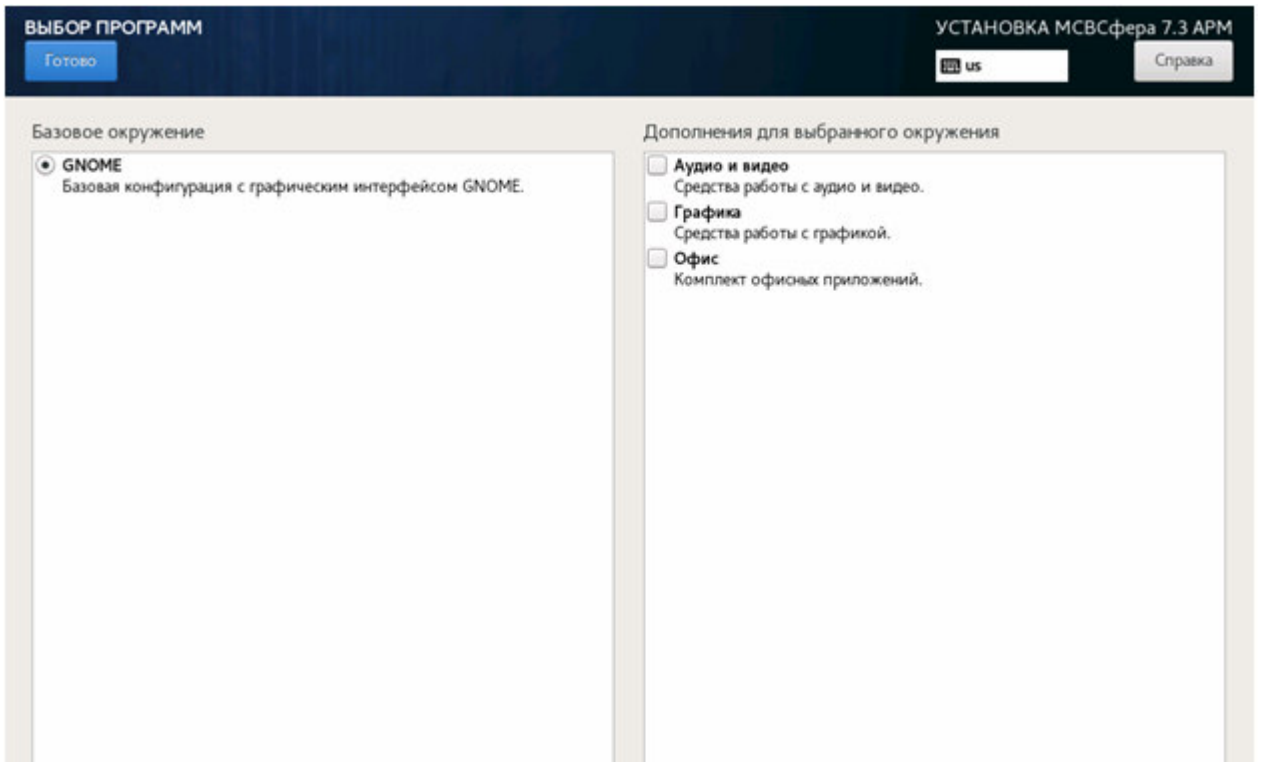


Снимок экрана 6 - Языковая поддержка

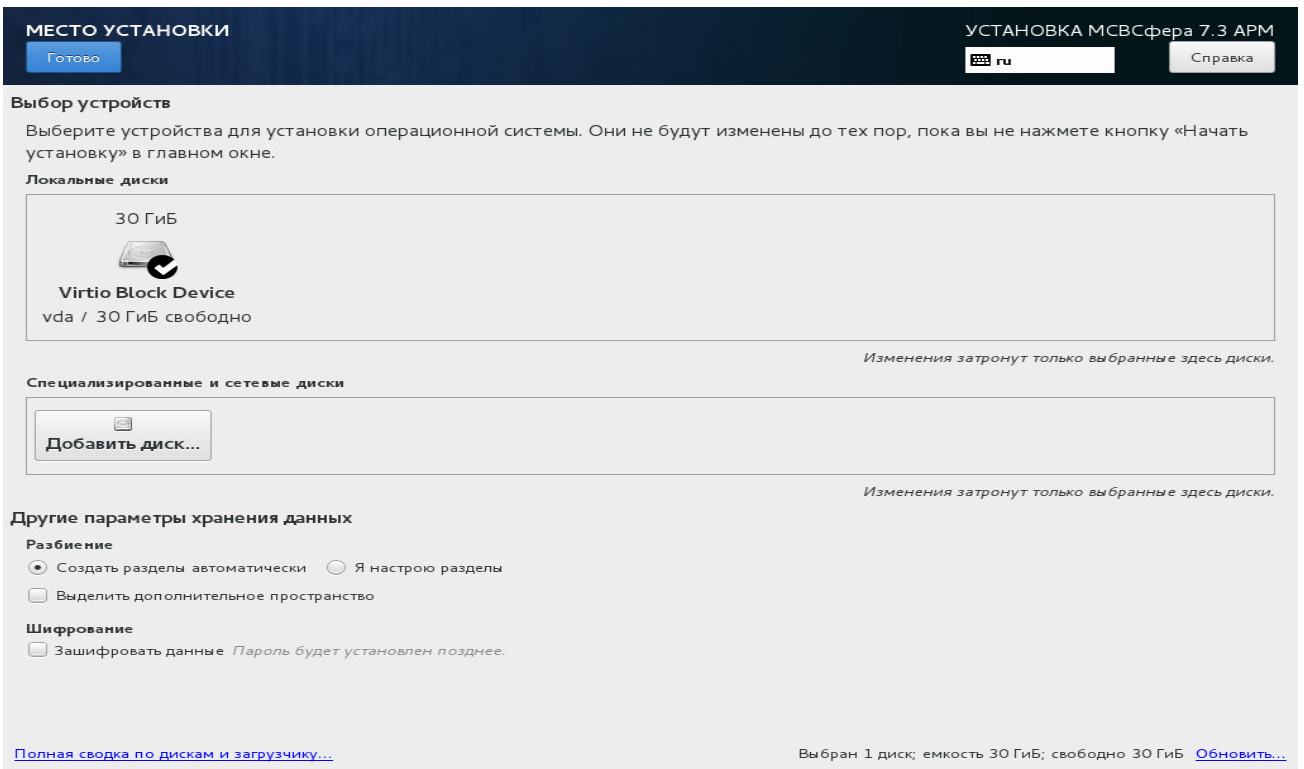


Снимок экрана 7 - Источник установки

Изм	Лист	№ докум	Подп	Дата

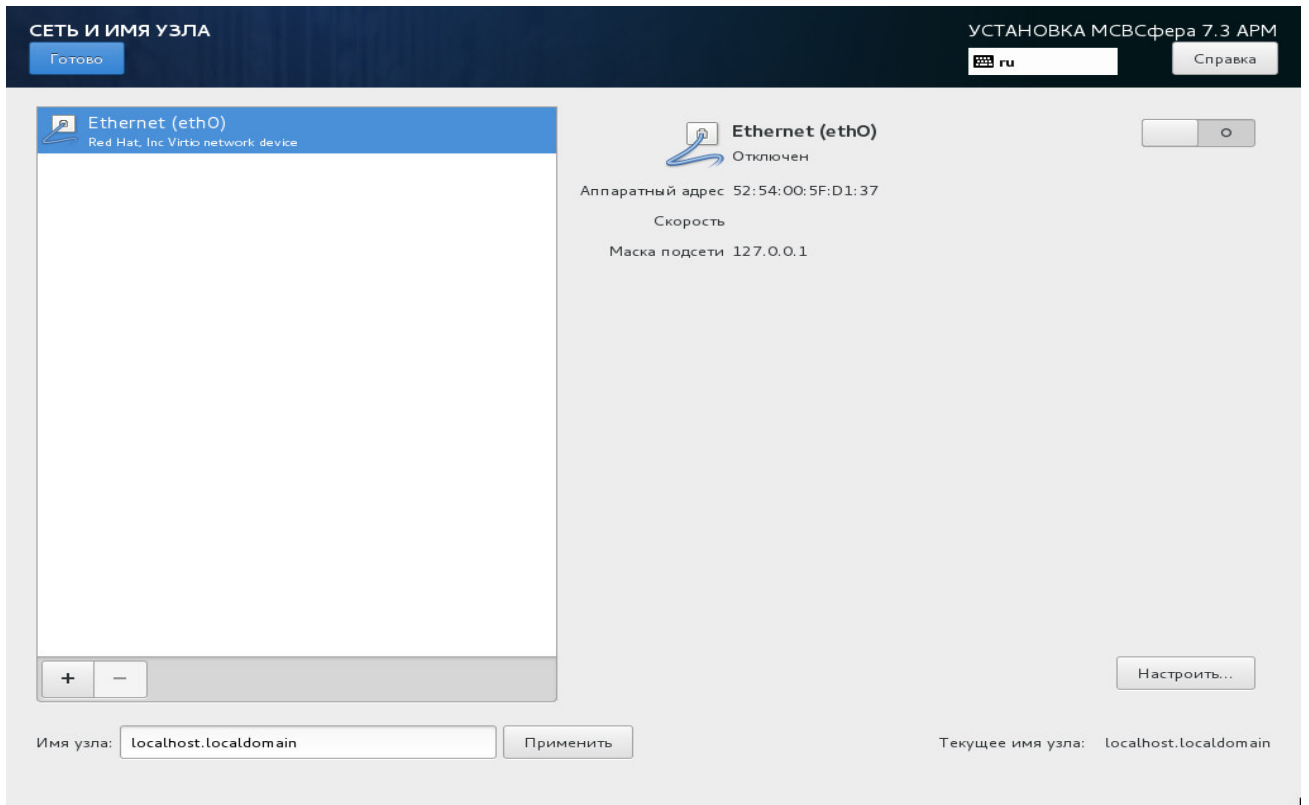


Снимок экрана 8 - Выбор программ

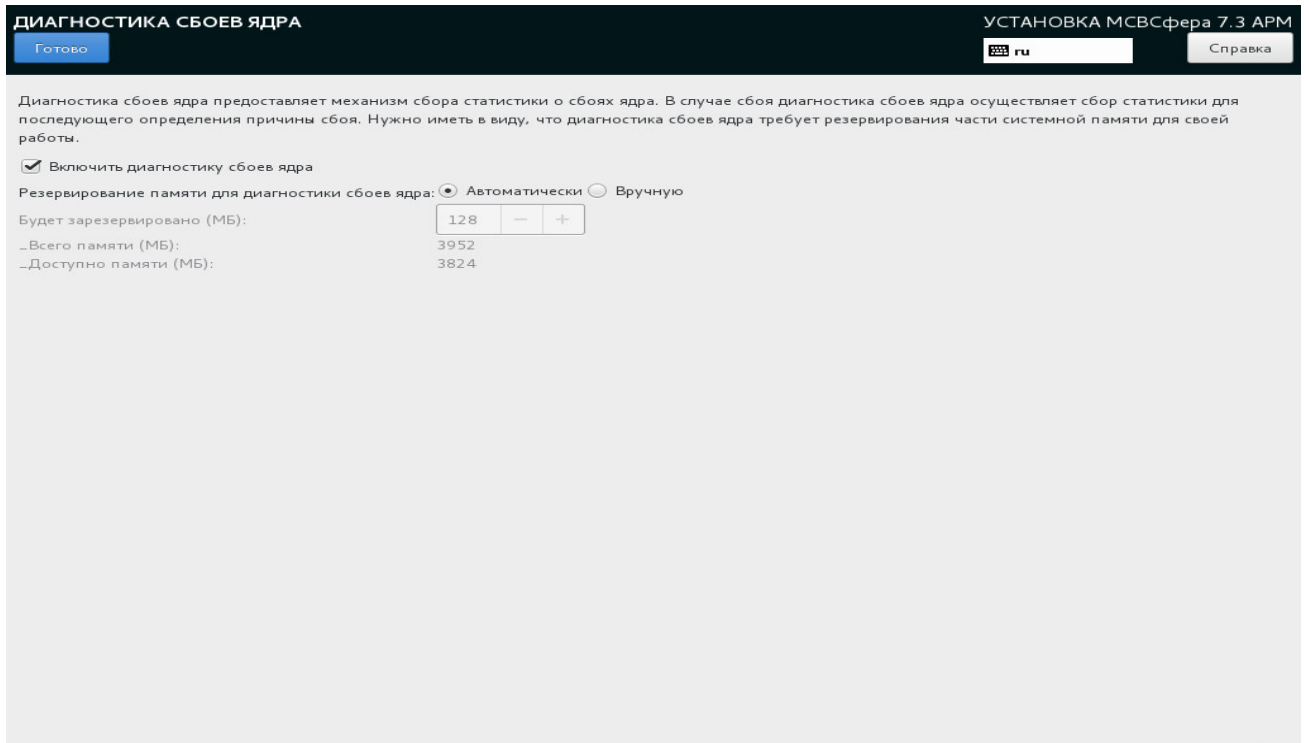


Снимок экрана 9 - Место установки

Изм	Лист	№ докум	Подп	Дата

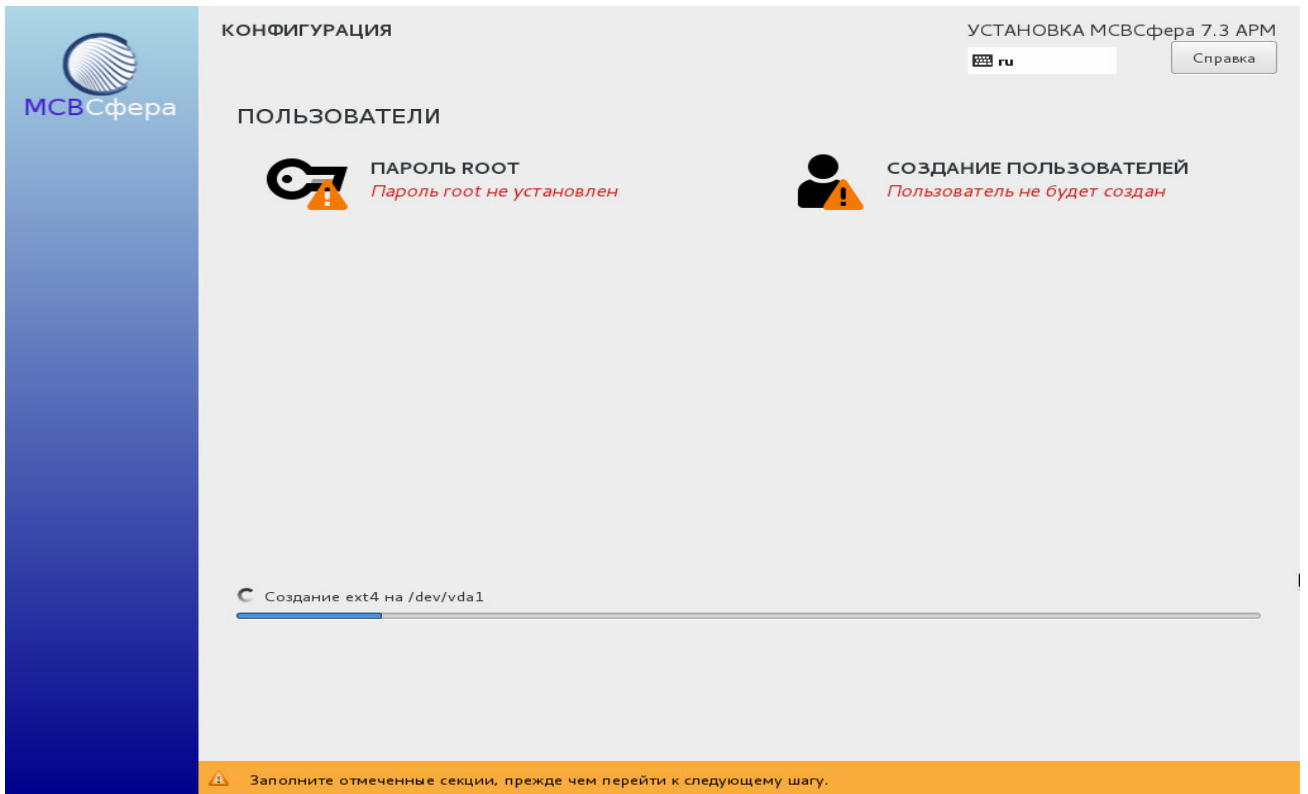


Снимок экрана 10 - Сеть и имя узла

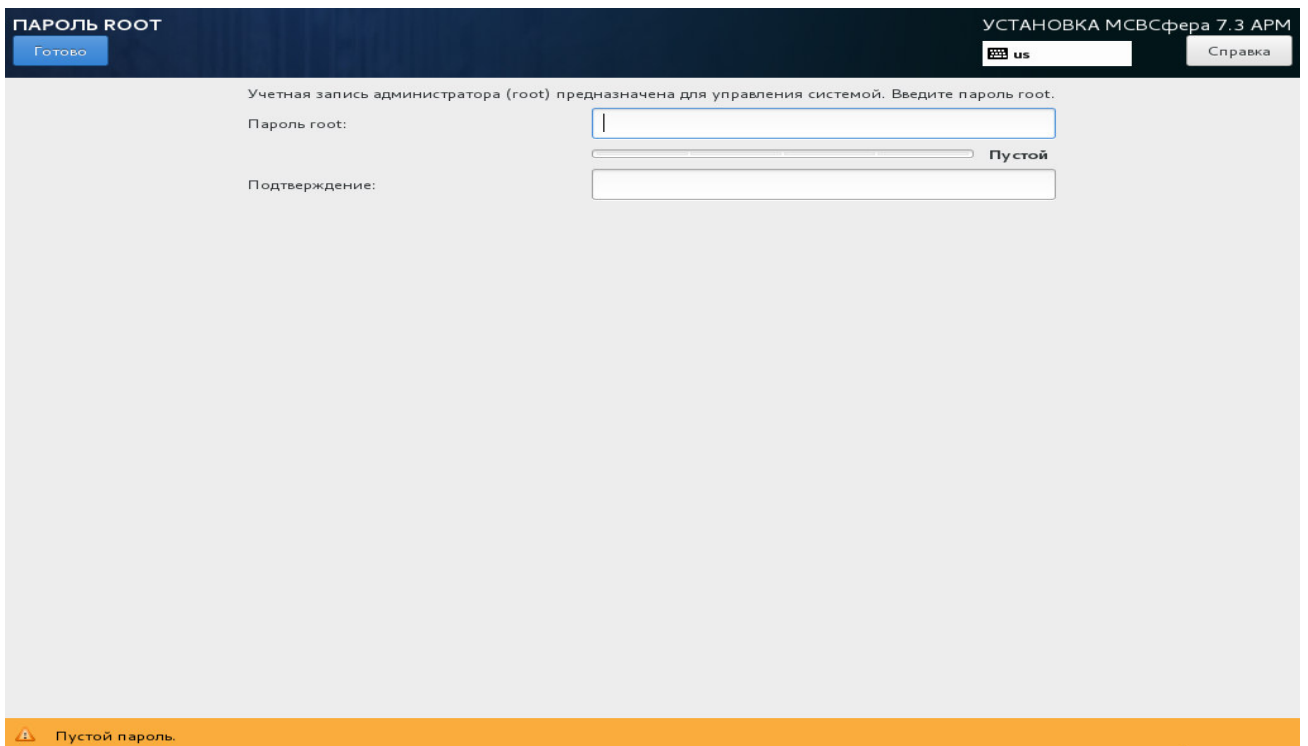


Снимок экрана 11 - Диагностика сбоев ядра

Изм	Лист	№ докум	Подп	Дата



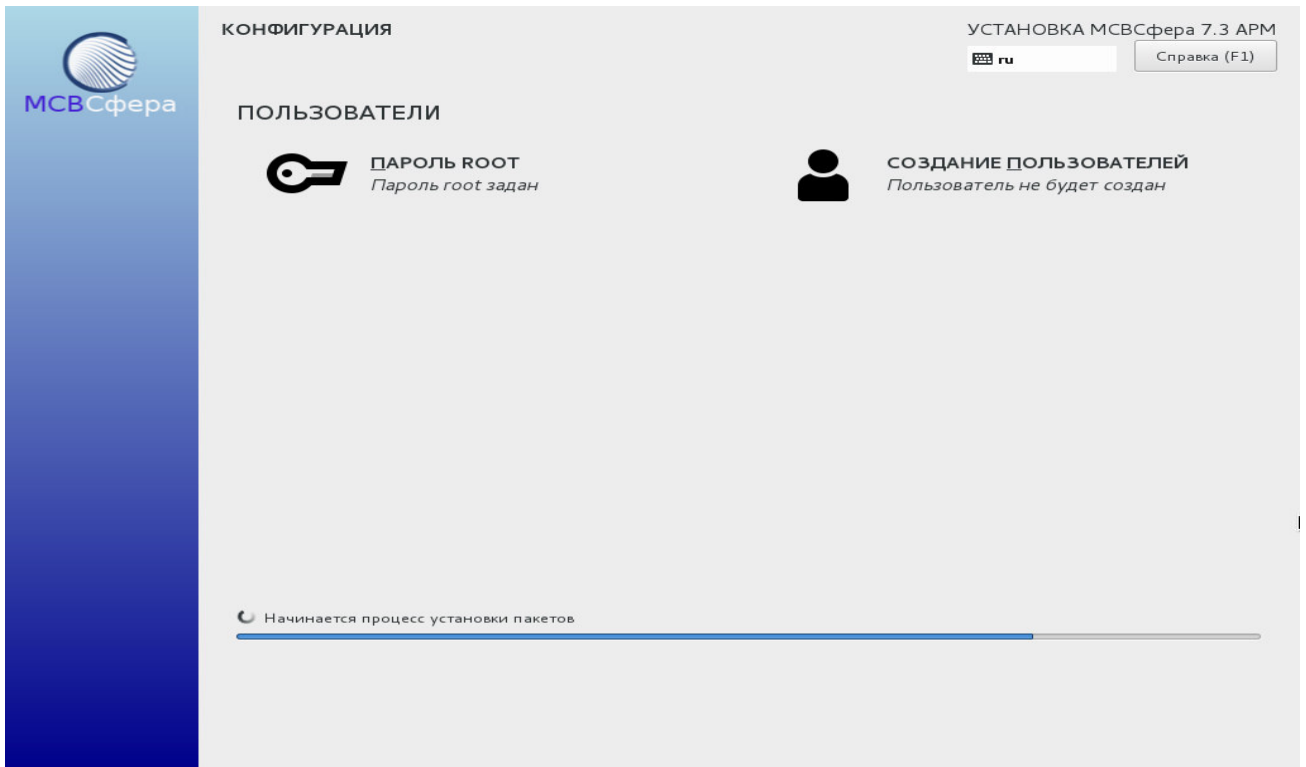
Снимок экрана 12 - Пользователи



Снимок экрана 13 - Пароль root

Изм	Лист	№ докум	Подп	Дата





Снимок экрана 14 - Создание пользователей

Снимок экрана 15 - Создание пользователя

Изм	Лист	№ докум	Подп	Дата

## 2 ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ

Средства идентификации и аутентификации предоставляют возможности идентификации объектов доступа, идентификации и проверки подлинности субъектов доступа при входе в систему и при доступе к защищаемым объектам, управления идентификаторами, в том числе их создания, присвоения и уничтожения, управления аутентификационными данными, в том числе их инициализации, защищенного хранения, блокирования и разблокирования, проверки соответствия аутентификационной информации заданной метрике качества, защиты обратной связи при вводе аутентификационной информации, а также другие возможности.

### 2.1 Утилита useradd

Утилита useradd позволяет добавить учетную запись нового пользователя. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-c, --comment. Любая текстовая строка. Используется как поле для имени и фамилии пользователя, длина этого поля не должна превосходить 128 символов;

-b, --base-dir. Базовый системный каталог по умолчанию, если другой каталог не указан с помощью параметра "-d". Базовый каталог объединяется с именем учётной записи для определения домашнего каталога;

-d, --home. Для создаваемого пользователя в качестве начального каталога будет использован базовый каталог. По умолчанию это значение получается объединением имени пользователя с базовым каталогом и используется как имя домашнего каталога;

-d, --home-dir. Задать домашний каталог нового пользователя. Если данная опция не используется, то в качестве домашнего каталога выбирается каталог типа /базовый\_системный\_каталог/имя\_пользователя;

-D, --defaults. Вывести значения стандартных опций;

-e, --expiredate. Дата блокировки учётной записи пользователя. Задаётся в формате ГГГГ-ММ-ДД;

-f, --inactive. Число дней, которые должны пройти после окончания срока действия пароля, чтобы учётная запись заблокировалась. Если указано значение 0, то учётная запись блокируется сразу после окончания срока действия пароля, а при значении -1 данная возможность не используется. По умолчанию используется значение -1;

Изм	Лист	№ докум	Подп	Дата

-g, --gid. Название группы нового пользователя или её идентификационный номер. Указываемое название группы или её номер должны существовать в системе;

-G, --groups. Список дополнительных групп, в которых числится пользователь. Перечисление групп осуществляется через запятую без промежуточных пробелов. На указанные группы действуют те же ограничения, что и для группы, указанной в опции -g;

-m, --create-home. Создает начальный домашний каталог нового пользователя, если он еще не существует. Если каталог уже существует, добавляемый пользователь должен иметь права на доступ к указанному каталогу;

-M, --no-create-home. Позволяет не создавать домашний каталог нового пользователя;

-K, --key — используется для изменения значений по умолчанию для параметров, хранимых в конфигурационном файле /etc/login.defs;

-N, --no-user-group. Позволяет добавить нового пользователя в группу, указанную в опции -g или заданную по умолчанию в конфигурационном файле /etc/default/useradd, не создавая группу, название которой совпадает с именем нового пользователя. Если опции -g, -N, -U не указаны, то настройки групп по умолчанию определяются в конфигурационном файле /etc/login.defs;

-o, --non-unique. Позволяет создать учётную запись с уже имеющимся, не уникальным идентификатором;

-p, --password. Позволяет задать новое зашифрованное значение пароля для учетной записи;

-r, --system. Позволяет создать системную учётную запись. По умолчанию для данной категории учетных записей домашний каталог не создаётся вне зависимости от значения соответствующего параметра конфигурационного файла /etc/login.defs . Для создания домашнего каталога системного пользователя необходимо вместе с опцией -r задать опцию -m;

-s, --shell. Полный путь к программе, используемой в качестве начального командного интерпретатора для пользователя сразу после регистрации. Длина этого поля не должна превосходить 256 символов. Если задать пустое значение, то будет использоваться оболочка по умолчанию;

-u, --uid. Позволяет задать идентификационный номер (численное неотрицательное значение идентификатора) пользователя. Это значение должно быть уникальным, если не задействована опция -o;

Изм	Лист	№ докум	Подп	Дата

-U, --user-group — позволяет создать группу, название которой совпадает с именем пользователя, присоединив данного пользователя к этой группе;

-h, --help — показать краткую справку об утилите.

Например, для создания пользователя *user* и задания для него основной группы *users* и двух дополнительных групп *ftp* и *developers*, к которым он будет приписан, необходимо выполнить команду:

```
useradd -g users -G ftp,developers user
```

## 2.2 Утилита `usermod`

Утилита `usermod` позволяет изменить данные существующей учетной записи пользователя. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-a, --append. Добавить пользователя в дополнительную группу. Следует использовать только вместе с параметром "-G";

-c, --comment. Новое значение поля комментария;

-d, --home. Новый домашний каталог учетной записи. Если указан параметр "-m", то содержимое текущего домашнего каталога будет перемещено в новый домашний каталог, который будет создан, если он ещё не существует;

-e, --expiredate. Установить дату окончания действия учетной записи в формате ГГГГ-ММ-ДД;

-f, --inactive. Установить пароль после окончания срока действия учетной записи в INACTIVE. Если указано значение 0, то учётная запись блокируется сразу после окончания срока действия пароля, при значении -1 данная возможность не используется. По умолчанию используется значение -1;

-g, --gid. Принудительно назначить первичную группу;

-G, --groups. Список дополнительных групп;

-l, --login. Новое значение учетной записи;

-L, --lock. Заблокировать пароль пользователя. Это делается помещением символа '!' в начало зашифрованного пароля, что приводит к его блокировке. Не следует использовать этот параметр вместе с "-p" или "-U";

Изм	Лист	№ докум	Подп	Дата

-m, --move-home. Переместить содержимое домашнего каталога пользователя в новое место. Если новый домашний каталог не существует, то он создаётся автоматически. Данная опция используется только вместе с опцией "-d".

-o, --non-unique. При использовании с параметром "-u", этот параметр позволяет указывать не уникальный числовой идентификатор пользователя;

-p, --password. Задать новый зашифрованный пароль для учетной записи;

-s, --shell. Задать новую оболочку для учетной записи;

-u, --uid. Новый идентификационный номер для учетной записи;

-U, --unlock. Разблокировать учетную запись.

Например, для изменения срока действия учетной записи пользователя с идентификатором *user6* необходимо выполнить команду:

```
usermod -e 2020-05-01 user6
```

где 2020-05-01 - дата истечения срока действия учетной записи в формате ГГГГ-ММ-ДД, а изменение идентификатора пользователя может быть сделано следующим образом:

```
[root@localhost user]# useradd user6
[root@localhost user]#
[root@localhost user]# id user6
uid=1004(user6) gid=1004(user6) группы=1004(user6)
[root@localhost user]#
[root@localhost user]# usermod -l user7 user6
[root@localhost user]#
[root@localhost user]# id user7
uid=1004(user7) gid=1004(user6) группы=1004(user6)
[root@localhost user]#
```

Снимок экрана 16 – Изменение идентификатора пользователя

### 2.3 Утилита *userdel*

Утилита *userdel* позволяет удалить существующую учетную запись пользователя. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-f, --force. С этой опцией учётная запись будет удалена, даже если пользователь в этот момент работает в системе. Она также заставляет утилиту удалить домашний каталог пользователя и почтовый ящик, даже если другой пользователь использует тот же домашний каталог или если почтовый ящик не принадлежит данному пользователю. Этот параметр опасно использовать, он может привести систему в нерабочее состояние;

Изм	Лист	№ докум	Подп	Дата

-r, --remove. Файлы в домашнем каталоге пользователя будут удалены вместе с самим домашним каталогом и почтовым ящиком. Пользовательские файлы, расположенные в других файловых системах, нужно искать и удалять вручную;

-n. Задаёт, сколько месяцев идентификатор пользователя должен устаревать перед повторным использованием. Задайте -1, чтобы указать, что идентификатор пользователя никогда не должен использоваться повторно. Задайте 0, чтобы указать, что идентификатор пользователя можно немедленно повторно использовать. Если опция -n не задана, то идентификатор будет устаревать стандартное количество месяцев перед повторным использованием.

-h, --help - показать краткую справку.

Например, удаление администратором пользователя *user7* с помощью утилиты `userdel` может быть сделано следующим образом:

```
[root@localhost user]# userdel -r user7
[root@localhost user]#
[root@localhost user]# cat /etc/passwd | grep user7
[root@localhost user]#
[root@localhost user]# ls /home
```

Снимок экрана 17 – Удаление пользователя

## 2.4 Утилита `groupadd`

Утилита `groupadd` позволяет добавить группу пользователей. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-f. Вернуть статус успешного выполнения, если группа уже существует. Если используется вместе с параметром "-g" и указанный идентификатор группы уже существует, то выбирается другой уникальный идентификатор группы, то есть параметр "-g" игнорируется;

-g. Числовое значение идентификатора группы. Значение должно быть уникальным, если не задан параметр "-o". Значение должно быть не отрицательным. По умолчанию берётся значение больше 999 и больше идентификатора любой другой группы. Значения от 0 и до 999 обычно зарезервированы под системные группы;

-K. Изменить значения по умолчанию для параметров, которые хранятся в конфигурационном файле `/etc/login.defs`;

-o. Разрешить добавление группы с не уникальным идентификатором;

-r, --system. Создать системную группу;

-h, --help. Показать краткую справку и закончить работу.

Изм	Лист	№ докум	Подп	Дата

Например, для создания группы `group2` с числовым значением идентификатора 8285 необходимо выполнить команду:

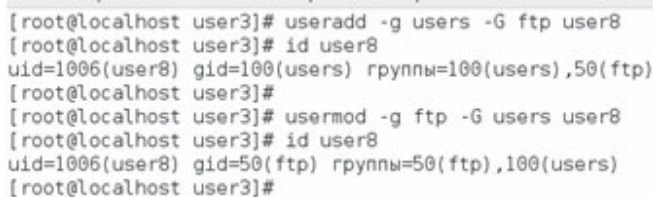
```
groupadd group2 -g 8285
```

## 2.5 Утилита `groupmod`

Утилита `groupmod` позволяет изменить существующую группу пользователей. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- g, --gid. Изменить идентификатор группы;
- n, --new-name. Изменить имя группы;
- o, --non-unique. Позволяет использовать не уникальный идентификатор группы;
- p, --password. Позволяет изменить зашифрованное значение пароля;
- h, --help. Показать краткую справку и закончить работу.

Например, добавление и изменение администратором групп может быть сделано следующим образом:



```
[root@localhost user3]# useradd -g users -G ftp user8
[root@localhost user3]# id user8
uid=1006(user8) gid=100(users) группы=100(users),50(ftp)
[root@localhost user3]#
[root@localhost user3]# usermod -g ftp -G users user8
[root@localhost user3]# id user8
uid=1006(user8) gid=50(ftp) группы=50(ftp),100(users)
[root@localhost user3]#
```

Снимок экрана 18 - Добавление и изменение групп

## 2.6 Утилита `groupdel`

Утилита `groupdel` позволяет удалить существующую группу пользователей, т.е. удалить определение группы из системы путем удаления записи о соответствующей группе из файла `/etc/group`. Однако, она не удаляет идентификатор группы из файла паролей. Удаленный идентификатор действует для всех файлов и каталогов, которые его имели.

Например, для удаления группы с именем `group3` необходимо выполнить следующую команду:

```
groupdel group3
```

Изм	Лист	№ докум	Подп	Дата

## 2.7 Утилита `passwd`

Утилита `passwd` позволяет создать и изменить пароль пользователя, в том числе заблокировать учетную запись пользователя.

Обычный пользователь может изменить пароль только своей учётной записи, суперпользователь `root` может изменить пароль любой учётной записи.

При изменении пароля проверяется информация об устаревании пароля, чтобы убедиться, что пользователю разрешено изменять пароль в настоящий момент. Если выяснится, что не разрешено, то утилита не производит изменение пароля и завершает работу.

При изменении пароля пользователь должен будет сначала ввести старый пароль, если он был. Введенное пользователем значение старого пароля зашифровывается и сравнивается со значением зашифрованного текущего пароля. Затем пользователю необходимо будет дважды ввести новый пароль. Значение второго ввода сравнивается с первым и они должны совпасть. После этого пароль тестируется на сложность подбора, т.е. его значение не должно быть легко угадываемым.

Утилита поддерживает следующий набор опций:

-a, --all. Эту опцию можно использовать только вместе с -S для вывода статуса всех пользователей;

-d, --delete. Удалить пароль пользователя (сделать его пустым). Это быстрый способ заблокировать пароль учётной записи;

-e, --expire. Немедленно сделать пароль устаревшим. Это заставит пользователя изменить пароль при следующем входе в систему;

-i, --inactive. Эта опция используется для блокировки учётной записи по прошествии заданного числа дней после устаревания пароля. То есть, если пароль устарел и прошло более указанных дней, то пользователь больше не сможет использовать свою учётную запись;

-l, --lock. Заблокировать указанную учётную запись. Эта опция блокирует учётную запись путем изменения значения пароля на такое, которое не может быть зашифрованным паролем;

-m, --mindays. Задать минимальное количество дней между сменой пароля. Нулевое значение этого поля указывает на то, что пользователь может менять свой пароль тогда, когда захочет;

Изм	Лист	№ докум	Подп	Дата



-S, --status. Показать состояние учётной записи. Информация о состоянии содержит семь полей. Первое поле содержит имя учётной записи. Второе поле указывает, заблокирована ли учётная запись, она без пароля или у неё есть рабочий пароль. Третье поле хранит дату последнего изменения пароля. В следующих четырёх полях хранятся минимальный срок, максимальный срок, период выдачи предупреждения и период неактивности пароля. Все эти сроки измеряются в днях;

-u, --unlock. Разблокировать указанную учётную запись. Этот параметр активирует учётную запись путем изменения пароля на прежнее значение, которое было перед использованием параметра -l;

-w, --warndays. Установить число дней выдачи предупреждения, перед тем как потребуется смена пароля;

-x, --maxdays. Установить максимальное количество дней, в течении которых пароль остаётся рабочим, после чего его надо будет изменить;

-h, --help. Показать краткую справку и закончить работу.

Например, задание пароля пользователю user4 с помощью утилиты passwd изображено на Снимке экрана 19, а вывод сведений о пароле изображен на Снимке экрана 20, где первое поле показывает имя пользователя, второе поле показывает статус пароля, третье поле отображает время последнего изменения пароля, четвертое и пятое поля показывают минимальный и максимальный срок действия пароля, шестое поле показывает срок вывода предупреждения, седьмое поле показывает срок деактивации пароля.

```
[root@localhost ~]# passwd user4
Изменяется пароль пользователя user4.
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[root@localhost ~]#
```

Снимок экрана 19 – Задание пароля

```
[root@localhost /]# passwd -S user4
user4 PS 2017-12-28 0 99999 7 -1 (Пароль задан, шифр SHA512.)
[root@localhost /]#
```

Снимок экрана 20 – Вывод сведений о пароле

Изм	Лист	№ докум	Подп	Дата

## 2.8 Утилита chage

Утилита chage позволяет установить дату завершения срока действия учетной записи пользователя, минимальный и максимальный срок действия пароля, дату завершения срока действия пароля, а также количество дней, в течение которых пользователю будут выводиться предупреждения о приближении завершения срока действия пароля. Командой chage может пользоваться только суперпользователь, за исключением использования ее с параметром "-l", который позволяет непривилегированным пользователям определить время, когда истекает их личный пароль или учетная запись. Режимы работы утилиты и выполняемые функции задаются набором опций, в том числе:

-m. Меняет значение mindays на минимальное число дней между сменой пароля. Значение 0 в этом поле обозначает, что пользователь может изменять свой пароль когда угодно;

-M. Меняет значение maxdays на максимальное число дней, в течении которых пароль будет действителен. Когда сумма maxdays и lastday меньше, чем текущий день, у пользователя будет запрошен новый пароль до начала работы в системе;

-d. Меняет значение lastday на день, когда пароль был изменен последний раз (число дней с 1 января 1970). Дата также может быть указана в формате ГГГГ-ММ-ДД;

-E. Используется для задания даты, с которой учетная запись пользователя станет недоступной, дата также может быть указана в формате ГГГГ-ММ-ДД;

-I. Используется для задания количества дней "неактивности", то есть дней, когда пользователь вообще не входил в систему, после которых его учетная запись будет заблокирована. Значение 0 отключает этот режим;

-W. Используется для задания числа дней, когда пользователю начнет выводиться предупреждение об истечении срока действия его пароля и необходимости его изменения.

Например, изменение срока действия пароля может быть сделано следующим образом:

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost user3]# chage -l user8
Последний раз пароль был изменён                : мар 12, 2018
Срок действия пароля истекает                    : никогда
Пароль будет деактивирован через                  : никогда
Срок действия учётной записи истекает            : никогда
Минимальное количество дней между сменой пароля  : 0
Максимальное количество дней между сменой пароля : 99999
Количество дней с предупреждением перед деактивацией пароля : 7
[root@localhost user3]#
[root@localhost user3]# passwd -x 20 user8
Устанавливаются параметры истечения срока действия для пользователя user8.
passwd: Успех
[root@localhost user3]#
[root@localhost user3]# chage -l user8
Последний раз пароль был изменён                : мар 12, 2018
Срок действия пароля истекает                    : apr 01, 2018
Пароль будет деактивирован через                  : никогда
Срок действия учётной записи истекает            : никогда
Минимальное количество дней между сменой пароля  : 0
Максимальное количество дней между сменой пароля : 20
Количество дней с предупреждением перед деактивацией пароля : 7
[root@localhost user3]#
```

Снимок экрана 21 - Изменение срока действия пароля

## 2.9 Утилита id

Утилита id позволяет получить сведения об указанном пользователе или о текущем пользователе, запустившем данную утилиту, если он не указал явно имя пользователя. По умолчанию выводятся числовые идентификаторы пользователя и группы, действующие идентификаторы пользователя и группы, а также идентификаторы других групп, в которых состоит пользователь. Режимы работы утилиты и выполняемые функции задаются набором опций, в том числе:

- g, --group. Выводит только подлинный числовой идентификатор группы;
- G, --groups. Выводит все подлинные числовые идентификаторы групп, в которых состоит пользователь;
- n, --name. Выводит действующие имена пользователей или групп.
- r, --real. Выводит подлинные числовые идентификаторы пользователей или групп;
- u, --user. Выводит только подлинный числовой идентификатор пользователя;
- version. Выводит информацию о версии утилиты и завершает работу;
- help. Выводит справку по этой утилите и завершает работу.

```
[user@localhost ~]$ id
uid=1000(user) gid=1000(user) группы=1000(user),100(users) контекст=user_u:user_r:user_t:s0
[user@localhost ~]$
[user@localhost ~]$ id -u
1000
[user@localhost ~]$
[user@localhost ~]$ id -g
1000
[user@localhost ~]$
```

Снимок экрана 22 – Сведения о пользователе

Изм.	Лист	№ докум	Подп	Дата

## 2.10 Конфигурационный файл /etc/login.defs

Конфигурационный файл /etc/login.defs позволяет задавать параметры, определяющие использование пользователями своих паролей (см. Снимок экрана 24), в том числе:

**PASS\_MAX\_DAYS** - определяет максимальный срок действия пароля, т.е. максимальное число дней, в течение которого действие пароля сохраняется. По истечении этого срока запускается процесс принудительной смены пароля. Если значение параметра не задано, то есть параметр закомментирован символом # или ему присвоено значение -1, то данное ограничение не установлено (отменяется);

**PASS\_MIN\_DAYS** - определяет минимальный срок между изменениями пароля, т.е. минимальное число дней между двумя последовательными изменениями пароля. Если значение параметра не задано, то есть параметр закомментирован символом # или ему присвоено значение -1, то данное ограничение не установлено (отменяется);

**PASS\_MIN\_LEN** - определяет минимальную допустимую длину задаваемого пароля;

**PASS\_WARN\_AGE** - определяет за сколько дней до истечения срока действия пароля начнется вывод предупреждения о необходимости его смены. Если значение параметра не задано, то есть параметр закомментирован символом # или ему присвоено значение -1, то данное ограничение не установлено (отменяется). Если значение параметра 0, то предупреждение о необходимости смены пароля будет выведено в день его устаревания.

Например, определение максимального количества дней действия пароля, равного 30 суткам, может быть выполнено следующим образом:

```
[root@localhost ~]# cat /etc/login.defs | grep PASS_MAX_DAYS
# PASS_MAX_DAYS Maximum number of days a password may be used.
PASS_MAX_DAYS 30
[root@localhost ~]#
```

Снимок экрана 23 – Определение срока действия пароля

## 2.11 Конфигурационный файл /etc/pam.d/system-auth

Конфигурационный файл /etc/pam.d/system-auth позволяет задавать настройки подключаемых модулей аутентификации (см. Снимок экрана 25). Каждая строка в нем представляет собой правило, состоящее из трёх обязательных полей и одного опционального. Поля разделены символом пробела. Порядок, в котором указаны правила, определяет очередность их проверки.

Изм	Лист	№ докум	Подп	Дата

```

#
# Please note that the parameters in this configuration file control the
# behavior of the tools from the shadow-utils component. None of these
# tools uses the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#

# *REQUIRED*
# Directory where mailboxes reside, _or_ name of file, relative to the
# home directory. If you _do_ define both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

# Password aging controls:
#
#     PASS_MAX_DAYS   Maximum number of days a password may be used.
#     PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#     PASS_MIN_LEN    Minimum acceptable password length.
#     PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN         1000
UID_MAX         60000
:█

```

Снимок экрана 24 – Фрагмент конфигурационного файла /etc/login.defs

Синтаксис правила:

type control module-path [module-arguments]

Поле type задаёт тип вызываемого модуля и может принимать одно из четырех допустимых значений:

auth - предназначен для аутентификации пользователя путём запроса и проверки его пароля;

account - используется для контроля доступа к сервису/приложению, например, может быть произведён запрос о том, не истёк ли срок действия аккаунта пользователя, разрешено ли пользователю работать с определённым сервисом в определённое время, хватает ли системных ресурсов для работы;

password - применяется для установки/изменения паролей;

session - управляет действиями пользователя в рамках активной сессии после его успешной аутентификации в системе.

Поле control задаёт действие, которое нужно выполнить после вызова модуля.

Доступно несколько действий:

Изм.	Лист	№ докум	Подп	Дата

`required` - модуль должен вернуть положительный ответ, если он возвращает отрицательный ответ, то пользователь будет уведомлён об этом только после того, как все остальные модули данного типа будут проверены;

`requisite` - требует от модуля положительный ответ, в случае получения отрицательного ответа последовательная проверка выполнения остальных правил моментально прекращается и пользователь получает сообщение об ошибке аутентификации;

`sufficient` - в случае, если ни один из модулей с действием `required` или `sufficient`, расположенных перед текущим, не вернул отрицательного ответа, текущий модуль вернёт положительный ответ и все последующие модули будут проигнорированы;

`optional` - результат проверки модуля важен только в том случае, если действие является единственным для данного модуля;

`include` - предназначается для добавления строк заданного типа из других файлов конфигурации из каталога `/etc/pam.d/` в файл конфигурации `/etc/pam.d/system-auth`. Название файла указывается в качестве аргумента действия;

Поле `module-path` задаёт путь к вызываемому модулю.

Поле `module-arguments` – дополнительные необязательные параметры модуля, необходимые для определения действий некоторых отдельных модулей в случае успешной авторизации. Так, если в конфигурационном файле найти строку, содержащую `pam_pwquality.so` и добавить в нее `minlen=8`, то будет установлена минимальная длина пароля равная 8-ми символам.

```
[root@localhost ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required     pam_limits.so
-session    optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required     pam_unix.so
[root@localhost ~]#
```

Снимок экрана 25 – Конфигурационный файл `/etc/pam.d/system-auth`

Изм.	Лист	№ докум	Подп	Дата

В качестве примера, сделаем блокировку учетной записи пользователя, который совершит определенное количество неудачных попыток входа в систему. Для этого внесем в файл `/etc/pam.d/system-auth` следующие изменения. Сначала допишем в секцию `auth` строку `"auth required pam_tally2.so deny=2 onerr=fail"`, т.е. подключим модуль `pam_tally2` и установим блокировку пользователя после двух (значение параметра `"deny"`) неудачных попыток входа. Затем в секции `account` добавим строку `"account required pam_tally2.so"` и прокомментируем строки вида: `"auth requisite pam_succeed_if.so uid >= 1000 quiet"` и `"auth required pam_deny.so"`, а потом строку `"auth sufficient pam_unix.so nullok try_first_pass"` заменим на `"auth required pam_unix.so nullok try_first_pass"`.

После этого пользователь, допустивший подряд две неверных попытки входа, на третьей получит сообщение о том, что его учетная запись заблокирована (см. Снимок экрана 26). И даже если четвертой попыткой он введет верный пароль, то все равно не получит доступ к системе.

```
[user@localhost ~]$ su user2
Пароль:
su: Сбой при проверке подлинности
[user@localhost ~]$ su user2
Пароль:
su: Сбой при проверке подлинности
[user@localhost ~]$ su user2
Пароль:
Учетная запись заблокирована как следствие неудачных попыток входа (всего -- 3).
su: Сбой при проверке подлинности
[user@localhost ~]$ su user2
Пароль:
Учетная запись заблокирована как следствие неудачных попыток входа (всего -- 4).
su: Сбой при проверке подлинности
[user@localhost ~]$
```

Снимок экрана 26 - Блокировка учетной записи пользователя

В качестве другого примера, настроим проверку паролей на сложность подбора через `pam_cracklib`. Для этого добавим или изменим строку `"password requisite pam_cracklib.so try_first_pass retry=3 type= minlen=6 dcredit=-2 ucredit=-3 lcredit=-2 ocredit=-1"`. Это значит, что после трех неуспешных попыток (`"retry=3"`) модуль вернет ошибку, минимальная длина для пароля - 6 символов (`"minlen=6"`), минимальное количество цифр - 2 (`"dcredit=-2"`), минимальное количество символов верхнего регистра - 3 (`"ucredit=-3"`), минимальное количество символов нижнего регистра - 2 (`"lcredit=-2"`), минимальное количество других символов - 1 (`"ocredit=-1"`). Удалим или прокомментируем строку `"password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type="`.

Изм	Лист	№ докум	Подп	Дата

Выполним команду `passwd` для смены пароля пользователя `user2` (см. Снимок экрана 27). Зададим пароль из трех символов и увидим сообщение "НЕУДАЧНЫЙ ПАРОЛЬ: слишком короткий". Зададим пароль из четырех символов, система выдаст сообщение "НЕУДАЧНЫЙ ПАРОЛЬ: короткий". Зададим пароль из шести символов (букв и цифр), в результате чего получим сообщение "НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой". После трех неуспешных попыток модуль вернет ошибку. Зададим пароль достаточной длины из одних цифр и получим сообщение "НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов" (см. Снимок экрана 28). Зададим пароль достаточной длины, содержащий все указанные требования, кроме включения в него отличных от алфавита и цифр символов, например "2QyfMOb4". Получим сообщение "НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой". Зададим пароль, соблюдая все установленные требования, например "2QyfM\*Ob4". Пароль будет успешно задан (см. Снимок экрана 29).

```
[user2@localhost user]$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль UNIX:
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком короткий
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: короткий
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
passwd: Использовано максимальное число попыток, заданное для службы
```

Снимок экрана 27 – Изменение значения пароля (1)

```
[user2@localhost user]$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль UNIX:
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком короткий
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: не содержит достаточное число РАЗЛИЧНЫХ символов
Новый пароль :
НЕУДАЧНЫЙ ПАРОЛЬ: слишком простой
passwd: Использовано максимальное число попыток, заданное для службы
[user2@localhost user]$
```

Снимок экрана 28 – Изменение значения пароля (2)

```
[user2@localhost user]$ passwd
Изменяется пароль пользователя user2.
Смена пароля для user2.
(текущий) пароль UNIX:
Новый пароль :
Повторите ввод нового пароля :
passwd: все данные аутентификации успешно обновлены.
[user2@localhost user]$ █
```

Снимок экрана 29 – Изменение значения пароля (3)

Изм	Лист	№ докум	Подп	Дата



## 2.12 Конфигурационный файл /etc/issue

Конфигурационный файл /etc/issue позволяет задать текстовое содержание уведомления пользователю перед началом его идентификации и аутентификации для входа в систему, например, с предупреждением о том, что в ней реализованы меры защиты информации и о необходимости соблюдения соответствующих правил обработки данных.

Традиционно в конфигурационном файле присутствуют опции выдачи сведений об операционной системе и ядре. Дополнительно можно добавить опции выдачи текущих даты и времени, количества работающих пользователей и некоторых других сведений.

## 2.13 Конфигурационный файл /etc/shadow

Конфигурационный файл /etc/shadow содержит сведения об учетных записях и паролях пользователей в виде строк со следующей структурой (см. Снимок экрана 30):

```
username:$id$salt$hashed:lastchanged:min:max:warn:inactive:expire
```

где:

username – имя пользователя;

id – алгоритм шифрования: 1 (алгоритм MD5), 5 (SHA-256), 6 (SHA-512);

salt – «соль», добавляемая к паролю строка из 10-20 случайных символов;

hashed – зашифрованный пароль;

lastchanged – дата последнего изменения пароля;

min – минимальное число дней между двумя последовательными сменами паролей;

max – срок действия пароля, т.е. максимальное число дней, в течение которого пароль будет активен;

warn – за какое количество дней до срока истечения действия пароля пользователь будет уведомлён о том, что его необходимо сменить;

inactive – количество дней после истечения срока действия пароля, спустя которое его учётная запись блокируется;

expire – число дней, прошедших с момента блокирования учетной записи.

Если после имени пользователя username вместо \$id\$salt\$hashed стоит символ \* либо последовательность из двух символов !!, то это означает, что попытки входа в систему от имени данного пользователя заблокированы.

Изм	Лист	№ докум	Подп	Дата

```
user:$6$iqGC8xaK0p01PJVz$u.FK7A6yQ2vy2BxLBr1sfvZ6RafcPguueQ6Sl rgjUVhwp39l9JCwGGMp1G/  
ZiR.tVF2pxnIz7N/RyJ.REac351::0:99999:7:::  
user2:$6$dUkd0AW0$XpKnU4TU0KeTAaMaPJCCcyA8ecRa8n6v.Ak0QbN5Bp0gb3U5ZHqZ/  
Hml0EkHeixdptZs0LqNhnVIgXHqdtEAC.:17561:0:99999:7:::  
user3:$6$.5H9EdMD$dJz1bLlv4lxZ56ArzJ9e/  
R3KZ1PPYKr7008FVJCq53902l/6i3EE6dPzM.mbmX1D66IuwbR0QAmxPuc0nIZ8Y1:17561:0:99999:7:::  
user6:$6$pkY8zQEY$qHYuS1sAt0yNydKR6/  
xAuuzgpZ9BwBmDeAw7bivqr1BaFYyH4MThpHgvY6gjRcz76P9x5rRQZfP8gK1gZY6yJ1:0:0:99999:7:::  
user5:$6$Dm5t4TVM$Dy3qwG6mlna0mx/  
H9rWpHclfuqqBgIfNmy0VfhEFAB3bU9RYswjgR6DnzGmdz9us.hc3kLWwqGRaWJLXFvb4w1:17569:0:99999:  
user4:$6$.1s8gvYh  
$JLwoidefcyoqR7wxzDj.kSdJAvySCDIGdjJ1aMUzVfeze0dDhJjBgbM0qRoRV8hvtX1Sia8fspGMuueveir/  
user8:!!$6$yKKG8VXi$WQACMhJgq13m0nQwtm0dMrIvHw59r73CyQPWY6ormJp3m0m4cq5IC0e.GMp/  
NTirjSTQKUHfo7Hpgzu3sIjSb1:0:0:20:7:::  
user9:$6$GGDs0EFk  
$Y9XVs8narlR.xsydPeEJcjDI8lubPPTKT5PgDwruIS.rTvBbwglHbxiWu0AZVSn4eDD0UCSuB3LEowu0VdX!
```

Снимок экрана 30 – Фрагмент конфигурационного файла /etc/shadow

Изм	Лист	№ докум	Подп	Дата

### 3 УПРАВЛЕНИЕ ДОСТУПОМ

Средства управления доступом предоставляют возможности ограничения количества одновременно предоставляемых параллельных сеансов доступа пользователей к системе, блокирования сеанса доступа пользователя в систему после истечения установленного периода времени бездействия или по его запросу, поддержки и сохранения атрибутов безопасности, связанных с информацией в процессе ее хранения и обработки, разделения полномочий пользователей и администраторов, обеспечивающих функционирование системы, реализации различных методов управления доступом, типов доступа и правил разграничения доступа, назначения приоритетов для использования субъектами доступа вычислительных ресурсов, квотирования предоставляемых вычислительных ресурсов, а также другие возможности.

#### 3.1 Утилита `chmod`

Утилита `chmod` позволяет устанавливать и изменять права доступа к файлам и директориям. Она принимает описания прав доступа в двух нотациях: численной и буквенной, описываемой ниже. В соответствии с буквенной нотацией пользователи, которые могут потенциально работать с файлом, разделяются на владельца (`u`), группу владельцев (`g`) и всех остальных пользователей (`o`), а файл может быть читаемым (`r`), записываемым (`w`) и исполняемым (`x`). Описание прав доступа начинается с символа, соответствующего типу пользователей, затем идет символ `+` для установки или символ `-` для снятия прав доступа, после чего описание заканчивается последовательностью символов, соответствующей правам доступа.

Например, для определения прав доступа, позволяющих читать и модифицировать файл *file*, может использоваться нотация:

```
chmod g+rw file
```

Для удаления всех прав доступа на директорию */directory* для группы и остальных пользователей может использоваться нотация:

```
chmod go-rwx /directory.
```

Утилита поддерживает также следующие опции:

`-R, --recursive`. Рекурсивное изменение прав доступа для директорий и их содержимого;

Изм	Лист	№ докум	Подп	Дата

-c, --changes. Подробно описывать действия для каждого файла, чьи права действительно изменяются;

-f, --silent, --quiet. Не выдавать сообщения об ошибке для файлов, чьи права не могут быть изменены;

-v, --verbose. Подробно описывать действие или отсутствие действия для каждого файла;

--version. Сообщить информацию о версии;

--help. Выдать справку.

Например, смена прав для файла *file1* с помощью утилиты *chmod* может быть сделана следующим образом:

```
[root@localhost user]# touch file1
[root@localhost user]#
[root@localhost user]# chmod 644 file1
[root@localhost user]#
[root@localhost user]# ls -l file1
-rw-r--r--. 1 root root 0 фев 19 11:55 file1
[root@localhost user]#
```

Снимок экрана 31 – Смена прав для файла

А определение для файла *file2* прав на чтение и запись для владельца и отсутствие доступа для остальных пользователей может быть сделано следующим образом:

```
[root@localhost user]# touch file2
[root@localhost user]#
[root@localhost user]# chmod 600 file2
[root@localhost user]#
[root@localhost user]# ls -l file2
-rw-----. 1 root root 0 фев 19 11:57 file2
[root@localhost user]#
```

Снимок экрана 32 – Определение прав для файла

Изм	Лист	№ докум	Подп	Дата

### 3.2 Утилита `chown`

Утилита `chown` позволяет назначить или изменить владельца файла или директории. Она поддерживает следующий набор опций:

`-R, --recursive`. Рекурсивное изменение прав доступа для директорий и их содержимого;

`-c, --changes`. Подробно описывать все изменения;

`-f, --silent, --quiet`. Не выдавать сообщения об ошибке;

`-v, --verbose`. Вывести подробное описание действий;

`--version`. Сообщить информацию о версии;

`--help`. Выдать справку.

Например, для назначения пользователя `user` владельцем файла `file` необходимо выполнить команду:

```
chown user file
```

Для рекурсивного обхода директории `directory` и назначения пользователя `user` владельцем всех вложенных файлов необходимо выполнить команду:

```
chown -R user directory
```

### 3.3 Утилита `chgrp`

Утилита `chgrp` позволяет изменить группу-владельца файла или директории. Она поддерживает следующий набор опций:

`-c, --changes`. Подробно описывать действия для каждого файла, чья группа действительно меняется;

`-f, --silent, --quiet`. Не выдавать сообщения об ошибке для файлов, чья группа не может быть изменена;

`-v, --verbose`. Подробно описывать действие или отсутствие действия для каждого файла;

`-R, --recursive`. Рекурсивное изменение группы для каталогов и всего их содержимого;

`--version`. Сообщить информацию о версии;

`--help`. Выдать справку.

Например, для изменения группы-владельца файла `file` на новую группу `new_group` необходимо выполнить команду:

```
chgrp new_group file
```

Изм	Лист	№ докум	Подп	Дата

### 3.4 Утилита `setfacl`

Утилита `setfacl` позволяет просматривать и изменять списки правил контроля доступа для файлов и директорий. Она поддерживает следующий набор опций:

- d. Установить правила контроля доступа по умолчанию;
- k. Удалить правила контроля доступа по умолчанию;
- s. Заменить правила контроля доступа заданными;
- m. Модифицировать правила контроля доступа;
- x. Удалить указанное правило контроля доступа;
- b. Удалить все правила контроля доступа;
- v. Вывод версии и выход;
- h, Вывод справки об использовании утилиты и выход.

Например, для удаления всех правил контроля доступа к файлу *file* необходимо выполнить команду:

```
setfacl -b file
```

### 3.5 Утилита `getfacl`

Утилита `getfacl` позволяет просматривать списки контроля доступа. Она поддерживает следующий набор опций:

- a, --access. Выводить список контроля доступа к файлам;
- d, --default. Выводить список контроля доступа по умолчанию;
- c, --omit-header. Не выводить заголовок с комментариями;
- e, --all-effective. Выводить комментарии с действующими правами доступа для каждого пользователя;
- E, --no-effective. Не выводить комментарии с действующими правами доступа ни для одного пользователя;
- R, --recursive. Делать рекурсивный обход директории и выводить списки контроля доступа для каждого файла и директории;
- v, --version. Вывести версию утилиты;
- h, --help. Вывести справочную информацию.

Например, определение списка контроля доступом для файла `cg.conf` может быть сделано следующим образом:

Изм	Лист	№ докум	Подп	Дата

```
[user@localhost ~]$ getfacl cg.conf
# file: cg.conf
# owner: user
# group: user
user::rwx
group::r-x
other::r-x
```

Снимок экрана 33 - Определение списка контроля доступом

Задание дополнительных компонентов списка контроля доступом для пользователя *user* и группы *user* по отношению к файлу *cg.conf* может быть сделано следующим образом:

```
[user@localhost ~]$ setfacl -m g:user:rwx cg.conf
[user@localhost ~]$ setfacl -m u:user:rwx cg.conf
[user@localhost ~]$ getfacl cg.conf
# file: cg.conf
# owner: user
# group: user
user::rwx
user:user:rwx
group::r-x
group:user:rwx
mask::rwx
other::r-x
```

Снимок экрана 34 - Переопределение списка контроля доступом

Модификация администратором списков контроля доступа для файлов, владельцем которых он является, может быть сделано следующим образом.

```
[root@localhost ~]# setfacl -m u:user:rwx ~/file2
[root@localhost ~]#
[root@localhost ~]# getfacl ~/file2
getfacl: Removing leading '/' from absolute path names
# file: root/file2
# owner: root
# group: root
user::rw-
user:user:rwx
group::r--
mask::rwx
other::r--

[root@localhost ~]#
```

Снимок экрана 35 - Модификация списков контроля доступа

Изм	Лист	№ докум	Подп	Дата

Модификация администратором списков контроля доступа для файлов, владельцем которых он не является, может быть сделано следующим образом.

```
[root@localhost ~]# setfacl -m u:user:rwx /home/user3/file2
[root@localhost ~]# setfacl -m u:user:rwx /home/user3/dir2/
[root@localhost ~]#
[root@localhost ~]# getfacl /home/user3/file2
getfacl: Removing leading '/' from absolute path names
# file: home/user3/file2
# owner: user3
# group: user3
user::rwx
user:user:rwx
group:---
mask::rwx
other:---

[root@localhost ~]# getfacl /home/user3/dir2/
getfacl: Removing leading '/' from absolute path names
# file: home/user3/dir2/
# owner: user3
# group: user3
user::rwx
user:user:rwx
group:---
mask::rwx
other:---

[root@localhost ~]# █
```

Снимок экрана 36 - Модификация списков контроля доступа

Удаление администратором списков контроля доступа для объектов, владельцем которых он является, может быть сделано следующим образом.

```
[root@localhost ~]# setfacl -b ~/file2
[root@localhost ~]# getfacl ~/file2
getfacl: Removing leading '/' from absolute path names
# file: root/file2
# owner: root
# group: root
user::rw-
group::r--
other::r--

[root@localhost ~]# █
```

Снимок экрана 37 – Удаление администратором списков контроля доступа

Изм	Лист	№ докум	Подп	Дата



Удаление администратором списков контроля доступа для объектов, владельцем которых он не является, может быть сделано следующим образом.

```
[root@localhost ~]# setfacl -b /home/user3/file2
[root@localhost ~]# getfacl /home/user3/file2
getfacl: Removing leading '/' from absolute path names
# file: home/user3/file2
# owner: user3
# group: user3
user::rwx
group::---
other::---
```

[root@localhost ~]# █

Снимок экрана 38 – Удаление администратором списков контроля доступа

Пользователь, не обладающий полномочиями администратора, не может удалять списки контроля доступа, которые он не создавал:

```
[root@localhost user]# touch file2
[root@localhost user]# ls -l file2
-rw-r--r--. 1 root root 0 фев 26 15:34 file2
[root@localhost user]# setfacl -m u:user2:rwx file2
[root@localhost user]# getfacl file2
# file: file2
# owner: root
# group: root
user::rw-
user:user2:rwx
group::r--
mask::rwx
other::r--

[root@localhost user]# exit
exit
[user@localhost ~]$ setfacl -b file2
setfacl: file2: Операция не позволена
[user@localhost ~]$ setfacl -x user2 file2
setfacl: file2: Операция не позволена
[user@localhost ~]$ █
```

Снимок экрана 39 – Попытка удаления списков контроля доступа

Изм	Лист	№ докум	Подп	Дата

### 3.6 Утилита seinfo

Утилита seinfo позволяет пользователю запрашивать политику SELinux. Режимы работы утилиты и выполняемые функции задаются набором опций, в том числе:

- c, --classes. Вывести список классов объектов;
- t, --types. Вывести список типов идентификаторов;
- a, --attribs. Вывести список атрибутов типа;
- r, --roles. Вывести список ролей;
- u, --users. Вывести список пользователей;
- b, --boolean. Вывести список условных логических выражений;
- S, --sensitivities. Вывести список чувствительности;
- C, --categories. Вывести список категорий;
- n, --netifcon. Вывести список контекстов;
- o, --nodecon. Вывести список контекстов узлов;
- p, --portcon. Вывести список контекстов портов;
- i, --initialsid. Вывести список начальных идентификаторов безопасности;
- A, --all. Вывести все вышеперечисленное;
- v, --version. Вывести информацию о версии и выйти;
- h, --help. Показать справку и выйти.

### 3.7 Утилита setenforce

Утилита setenforce позволяет устанавливать режим выполнения политики SELinux, а именно: Enforcing (или 1), чтобы перевести SELinux в принудительный режим, Permissive (или 0), чтобы перевести SELinux в разрешительный режим.

### 3.8 Утилита setfiles

Утилита setfiles позволяет устанавливать контекст безопасности SELinux для файлов. Она поддерживает следующий набор опций:

- c. Проверить соответствие контекста тому, что определен в двоичном файле политики;
- d. Показать, какая спецификация соответствует каждому файлу;
- l. Отобразить изменения меток в системном логе;
- n. Не менять метки файлов;

Изм	Лист	№ докум	Подп	Дата

- q. Подавить вывод, не относящийся к ошибкам;
- r. Использовать альтернативный путь к корневой директории;
- e. Задать директорию, которую нужно исключить из обработки;
- F. Принудительно установить контекст;
- v. Показать изменения меток файлов, если изменился тип или роль;
- vv. Показать изменения меток файлов, если изменился тип, роль или пользователь;
- W. Вывести предупреждения, если встретятся спецификации, которым не соответствует ни один файл.

### 3.9 Утилита `restorecon`

Утилита `restorecon` позволяет восстановить заданный по умолчанию контекст безопасности SELinux для файлов. Она поддерживает следующий набор опций:

- i. Игнорировать несуществующие файлы;
- f. Задать список файлов, которые будут обработаны;
- e. Задать директорию, которую нужно исключить из обработки;
- o. Сохранить список файлов с некорректным контекстом;
- v. Показать изменения меток файлов;
- vv. Показать изменения меток файлов, если изменился тип, роль или пользователь.

### 3.10 Утилита `chcon`

Утилита `chcon` позволяет изменить контекст безопасности SELinux для файлов. Она поддерживает следующий набор опций:

- u. Задать пользователя в назначаемом контексте безопасности;
- r. Задать роль в назначаемом контексте безопасности;
- t. Задать тип в назначаемом контексте безопасности;
- l. Задать диапазон в назначаемом контексте безопасности;
- R. Рекурсивно обрабатывать файлы и каталоги;
- v. Выводить диагностические сообщения для каждого файла;
- v. Показать информацию о версии и выйти;
- h. Показать справку и выйти.

Изм	Лист	№ докум	Подп	Дата

Например, изменение контекста безопасности для файла *test* на *home\_bin\_t* может быть сделано следующим образом.

```
[root@localhost html]# chcon -t home_bin_t test
[root@localhost html]# ls -Z test
-rw-r--r--. root root user_u:object_r:home_bin_t:s0 test
[root@localhost html]#
[root@localhost html]#
```

Снимок экрана 40 – Изменение контекста безопасности

### 3.11 Утилита *edquota*

Утилита *edquota* позволяет редактировать пользовательские квоты для файловой системы. Режимы ее работы и выполняемые функции определяются набором опций, в том числе:

- u, --user. Изменить пользовательскую квоту;
- g, --group. Изменить групповую квоту;
- p, --prototype = protoname. Дублировать квоты прототипного пользователя, это обычный механизм, используемый для инициализации квот для групп пользователей;
- F, --format = имя-формата. Изменить квоту для указанного формата;
- f, --filesystem. Выполнять указанные операции только для заданной файловой системы, по умолчанию выполняется операция для всех файловых систем с квотой;
- t, --edit-period. Редактировать мягкие ограничения по времени для каждой файловой системы;
- T, --edit-times. Изменить время для пользователя или группы, когда принудительное ограничение установлено.

### 3.12 Конфигурационный файл */etc/profile*

Конфигурационный файл */etc/profile* используется для задания элементов окружения оболочки пользователя. Например, в нём определяются глобальные переменные:

*PATH* – переменная среды, используемая для указания оболочке списка каталогов, которые будут просматриваться при поиске исполняемых файлов;

*USER* – имя пользователя при входе в ОС;

Изм	Лист	№ докум	Подп	Дата

LOGNAME – то же, что и USER, некоторые программы считывают значение этой глобальной переменной вместо USER;

MAIL – имя файла, в который записывается локальная почта пользователя, а также его расположение;

HOSTNAME – имя хоста;

HISTSIZE – количество исполненных команд, сохраняемых в истории;

HISTCONTROL – политики в отношении команд, сохраняемых в истории. По умолчанию задано значение ignoredups, то есть команда, полностью совпадающая с одной из уже записанных в историю, не сохраняется. Если задать политику ignorespace, то будут игнорироваться как дублирующиеся команды, так и те, что начинаются с символа пробела.

Также в конфигурационном файле задаётся маска, используемая для определения конечных прав доступа для пользователя.

```
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

# It's NOT a good idea to change this file unless you know what you
# are doing. It's much better to create a custom.sh shell script in
# /etc/profile.d/ to make custom changes to your environment, as this
# will prevent the need for merging in future updates.

pathmunge () {
  case ":{PATH}:" in
    *:"$1":*)
      ;;
    *)
      if [ "$2" = "after" ] ; then
        PATH=$PATH:$1
      else
        PATH=$1:$PATH
      fi
  esac
}

if [ -x /usr/bin/id ]; then
  if [ -z "$EUID" ]; then
    # ksh workaround
    EUID=`/usr/bin/id -u`
    UID=`/usr/bin/id -ru`
  fi
  USER="`/usr/bin/id -un`"
  LOGNAME=$USER
  MAIL="/var/spool/mail/$USER"
fi
:
```

Снимок экрана 41 – Конфигурационный файл /etc/profile (1)

Изм	Лист	№ докум	Подп	Дата

```

# Path manipulation
if [ "$EUID" = "0" ]; then
    pathmunge /usr/sbin
    pathmunge /usr/local/sbin
else
    pathmunge /usr/local/sbin after
    pathmunge /usr/sbin after
fi

HOSTNAME=`/usr/bin/hostname 2>/dev/null`
HISTSIZE=1000
if [ "$HISTCONTROL" = "ignorespace" ]; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want umask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        fi
    fi
done

```

Снимок экрана 42 – Конфигурационный файл /etc/profile (2)

```

HISTSIZE=1000
if [ "$HISTCONTROL" = "ignorespace" ]; then
    export HISTCONTROL=ignoreboth
else
    export HISTCONTROL=ignoredups
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL

# By default, we want umask to get set. This sets it for login shell
# Current threshold for system reserved uid/gids is 200
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`/usr/bin/id -gn`" = "`/usr/bin/id -un`" ]; then
    umask 002
else
    umask 022
fi

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        if [ "${-#*i}" != "$-" ]; then
            . "$i"
        else
            . "$i" >/dev/null
        fi
    fi
done

unset i
unset -f pathmunge

rm /media/distrib/MSVSphere 2> /dev/null || true
ln -s /run/media/$USER/MSVSphere /media/distrib
(END)

```

Снимок экрана 43 – Конфигурационный файл /etc/profile (3)

Изм	Лист	№ докум	Подп	Дата

Например, определим время бездействия при локальной терминальной сессии равным двум минутам (120 с). Для этого в файле /etc/profile после строк следующего содержания:

```
HOSTNAME= '/usr/bin/hostname 2>/dev/null'
```

```
HISTSIZE=1000
```

Необходимо добавить строку "TMOUT=120".

Там же, в строке, имеющей следующее содержание:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE HISTCONTROL
```

необходимо добавить параметр TMOUT:

```
export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE TMOUT
HISTCONTROL
```

Для подтверждения вступления изменений в силу надо будет завершить сеанс и зарегистрироваться в системе заново. Тогда появится сообщение, что после двух минут бездействия время ожидания ввода вышло, в результате чего интерактивный сеанс был закрыт.



```
[user@localhost ~]$ su
Пароль:
[root@localhost user]# timed out waiting for input: auto-logout
[user@localhost ~]$
```

Снимок экрана 44 – Завершение сеанса по окончании времени бездействия

### 3.13 Конфигурационный файл /etc/security/limits.conf

Конфигурационный файл /etc/security/limits.conf может использоваться для задания модулю pam\_limits.so дополнительных ограничений. Для этого каждая его строка включает четыре группы параметров (см. Снимки экрана 45 и 46, по умолчанию все ограничения отключены - все строки закомментированы), которые перечислены и описаны ниже:

<domain>: имя пользователя, имя группы с синтаксисом @group, подстановочный знак \* для записи по умолчанию, подстановочный знак %, который также может использоваться с синтаксисом %group для ограничения maxlogin;

<type>: “soft” для установки мягких ограничений, “hard” для установки жестких ограничений;

<item>: core (ограничивает размер файла ядра в КБ), data (максимальный размер данных в КБ), fsize (максимальный размер файла в КБ), memlock (максимальное адресное пространство, предустановленное в памяти в КБ), nofile (максимальное количество открытых

Изм	Лист	№ докум	Подп	Дата

файлов), `rss` (максимальный размер резидентного набора в КБ), `stack` (максимальный размер стека в КБ), `cpu` (максимальное время процессора в MIN), `prcos` (максимальное количество процессов), `as` (ограничение адресного пространства в КБ), `maxlogins` (максимальное количество логинов для этого пользователя), `maxsyslogins` (максимальное количество входов в систему), `priority` (приоритет процессов пользователя), `locks` (максимальное количество блокировок файлов, которое может быть обеспечено пользователем), `sigpending` (максимальное количество ожидающих сигналов), `msgqueue` (максимальный объем памяти, используемый очередями сообщений POSIX в байтах), `nice` (приоритет для запуска процессов утилитой `nice`), `rtprio` (максимальный приоритет в реальном времени).

Например, ограничить число параллельных сеансов доступа для каждой учетной записи пользователя можно, добавив в конфигурационный файл строку следующего содержания: `username hard maxlogins 2`. Тогда, при условии, что пользователь `username` уже открыл локальную сессию (первый активный сеанс) и попытался зайти в систему через `ssh` соединение (потенциальный второй активный сеанс), ему будет выведено сообщение `Too many logins for 'username'` и второе соединение будет заблокировано.

```
# /etc/security/limits.conf
#
#This file sets the resource limits for the users logged in via PAM.
#It does not affect resource limits of the system services.
#
#Also note that configuration files in /etc/security/limits.d directory,
#which are read in alphabetical order, override the settings in this
#file in case the domain is the same or more specific.
#That means for example that setting a limit for wildcard domain here
#can be overridden with a wildcard setting in a config file in the
#subdirectory, but a user specific setting here can be overridden only
#with a user specific setting in the subdirectory.
#
#Each line describes a limit for a user in the form:
#
#<domain>          <type> <item> <value>
#
#Where:
#<domain> can be:
#   - a user name
#   - a group name, with @group syntax
#   - the wildcard *, for default entry
#   - the wildcard %, can be also used with %group syntax,
#       for maxlogin limit
#
#<type> can have the two values:
#   - "soft" for enforcing the soft limits
#   - "hard" for enforcing hard limits
#
#<item> can be one of the following:
#   - core - limits the core file size (KB)
#   - data - max data size (KB)
#   - fsize - maximum filesize (KB)
#   - memlock - max locked-in-memory address space (KB)
#
:█
```

Снимок экрана 45 – Конфигурационный файл `/etc/security/limits.conf` (1)

Изм	Лист	№ докум	Подп	Дата



```

# - "hard" for enforcing hard limits
#
#<item> can be one of the following:
# - core - limits the core file size (KB)
# - data - max data size (KB)
# - fsize - maximum filesize (KB)
# - memlock - max locked-in-memory address space (KB)
# - nofile - max number of open file descriptors
# - rss - max resident set size (KB)
# - stack - max stack size (KB)
# - cpu - max CPU time (MIN)
# - nproc - max number of processes
# - as - address space limit (KB)
# - maxlogins - max number of logins for this user
# - maxsyslogins - max number of logins on the system
# - priority - the priority to run user process with
# - locks - max number of file locks the user can hold
# - sigpending - max number of pending signals
# - msgqueue - max memory used by POSIX message queues (bytes)
# - nice - max nice priority allowed to raise to values: [-20, 19]
# - rtprio - max realtime priority
#
#<domain> <type> <item> <value>
#
#*          soft  core          0
#*          hard  rss           10000
#@student  hard  nproc          20
#@faculty  soft  nproc          20
#@faculty  hard  nproc          50
#ftp       hard  nproc          0
#@student  -     maxlogins      4

# End of file
(EN)

```

Снимок экрана 46 – Конфигурационный файл /etc/security/limits.conf (2)

### 3.14 Конфигурационный файл /etc/fstab

Конфигурационный файл /etc/fstab используется для настройки параметров монтирования различных блочных устройств, разделов на диске и файловых систем.

Он состоит из набора так называемых определений, каждое из которых занимает свою строку и состоит из шести полей, разделённых пробелами или символами табуляции:

```
fs_spec fs_file fs_vfstype fs_mntops fs_freq fs_passno
```

Поля предназначены для задания следующих параметров:

**fs\_spec** – физическое размещение файловой системы, по которому определяется конкретный раздел или устройство хранения для монтирования. Вместо указания размещения файловой системы явным образом можно воспользоваться её уникальным идентификатором UUID;

**fs\_file** – точка монтирования, куда монтируется корень файловой системы;

**fs\_vfstype** – тип файловой системы. Поддерживаются следующие типы: adfs, affs, autofs, coda, coherent, cramfs, devpts, efs, ext2, ext3, ext4, hfs, hpfs, iso9660, jfs, minix, msdos, nvpfs, nfs, ntfs, proc, qnx4, reiserfs, romfs, smbfs, sysv, tmpfs, udf, ufs, umsdos, vfat, xenix, xfs;

Изм	Лист	№ докум	Подп	Дата

`fs_mntops` – опции монтирования файловой системы. Основные опции: `defaults`, `noauto`, `user`, `owner`, `comment`, `nofail`;

`fs_freq` – предназначено для использования утилитой создания резервных копий в файловой системе. Возможные значения: 0 и 1, если указано 1, то утилита создаст резервную копию;

`fs_passno` – предназначено для использования программой `fsck` при необходимости проверки целостности файловой системы; возможные значения: 0, 1 и 2; значение 1 указывается только для корневой файловой системы (то есть файловой системы с точкой монтирования `/`); для остальных файловых систем для проверки утилитой `fsck` задаётся значение 2; 0 – проверка выполняться не будет;

По умолчанию конфигурационный файл включает (см. Снимок экрана 47):

`/dev/mapper/MSVSphere-root / xfs defaults 0 0` – файловая система `/dev/mapper/MSVSphere-root` примонтирована в каталог `/`, тип файловой системы – `xfs`, используемые опции – `defaults`, резервная копия данных не создаётся (`fs_freq=0`), проверка целостности файловой системы не выполняется (`fs_passno=0`);

`UUID=b1bfe9b0-96ea-4876-883c-a9f1b6c74b /boot ext4 defaults 1 2` – файловая система с идентификатором `b1bfe9b0-96ea-4876-883c-a9f1b6c74b` смонтирована в `/boot`, тип файловой системы – `ext4`, используемые опции – `defaults`, резервная копия данных создаётся (`fs_freq=1`), проверка целостности файловой системы выполняется (`fs_passno=2`);

`/dev/mapper/MSVSphere-swap swap defaults 0 0` – файловая система `/dev/mapper/MSVSphere-swap` является разделом подкачки `swap`, используемые опции – `defaults`, резервная копия данных не создаётся (`fs_freq=0`), проверка целостности файловой системы не выполняется (`fs_passno=0`).

```
[root@localhost ~]# cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Mon Oct 21 10:43:57 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/MSVSphere-root / xfs defaults 0 0
UUID=895605f5-871b-44f7-b687-e51ab27e1f5d /boot ext4 defaults 1 2
/dev/mapper/MSVSphere-swap swap swap defaults 0 0
[root@localhost ~]#
```

Снимок экрана 47 – Конфигурационный файл `/etc/fstab`

Изм	Лист	№ докум	Подп	Дата

## 4 РЕГИСТРАЦИЯ СОБЫТИЙ БЕЗОПАСНОСТИ

Средства регистрации событий безопасности предоставляют возможности включения и исключения событий безопасности в совокупность событий, подвергающихся регистрации, регистрации событий безопасности; предоставления регистрируемой информации в понятном и защищенном от несанкционированного доступа виде; обеспечения непрерывности процесса регистрации при превышении журналом регистрации определенного размера; выборочного просмотра, поиска, сортировки и упорядочения регистрируемой информации, изготовления соответствующих отчетов, а также другие возможности.

### 4.1 Утилита `auditctl`

Утилита `auditctl` позволяет формировать, добавлять или удалять правила регистрации событий безопасности. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-b `backlog`. Установить максимальное количество доступных для записи данных регистрации буферов, значение по умолчанию – 64;

--`backlog_wait_time`. Установить время ожидания до постановки новой партии данных регистрации событий безопасности в очередь и последующей их обработки при достижении предельного значения;

-e [0..2]. Установить флаг блокировки: 0 позволит на время отключить регистрацию, 1 позволит включить ее обратно, а 2 позволит защитить конфигурацию регистрации от изменений;

-f [0..2]. Установить способ обработки для флага `сбоя`. Эта опция позволяет определить, каким образом ядро будет обрабатывать критические ошибки. Значение по умолчанию: 1. Для систем с повышенными требованиями к безопасности, значение 2 может быть более предпочтительным;

-h. Краткая помощь по аргументам командной строки;

-i. Игнорировать ошибки при чтении правил из файла;

-l. Вывести список всех правил по одному правилу в строке;

Изм	Лист	№ докум	Подп	Дата

-k ключ. Установить на правило ключ фильтрации. Ключ фильтрации - это произвольная текстовая строка длиной не больше 31 символа. Ключ помогает уникально идентифицировать записи, генерируемые в ходе аудита за точкой наблюдения;

-m текст. Послать в систему регистрации событий пользовательское сообщение. Это возможно только из аккаунта учетной записи суперпользователя root;

-p [rlw|sla]. Установить фильтр прав доступа для точки наблюдения. r (чтение), w (запись), x (исполнение), a (изменение атрибута);

-r частота. Установить ограничение скорости выдачи сообщений в секунду (0 - нет ограничения). Если эта частота ненулевая, и она превышает в ходе аудита, флаг сбоя выставляется ядром для выполнения соответствующего действия. Значение по умолчанию: 0;

-R файл. Читать правила из файла. Правила должны быть расположены по одному в строке и в том порядке, в каком они должны исполняться. Владелец файла с правилами должен быть суперпользователь root, данный файл не должен быть доступен для чтения любым другим пользователям, в противном случае операция с опцией не будет позволена;

-s. Получить статус регистрации событий;

-a список, действие. Добавить правило с указанным действием к концу списка;

-A список, действие. Добавить правило с указанным действием в начало списка;

-d список, действие. Удалить правило с указанным действием из списка. Правило удаляется только в том случае, если полностью совпали и имя системного вызова и поля сравнения;

-D. Удалить все правила и точки наблюдения;

-c. Продолжить загружать правила, несмотря на появление ошибки. Таким образом можно отследить конечный результат загрузки правил. Если хотя бы одно из правил не загрузилось, код возврата будет ненулевой;

-S [Имя или номер системного вызова | all]. Любой номер или имя системного вызова может быть использован. Также возможно использование ключевого слова all. Если какой-либо процесс выполняет указанный системный вызов, то служба регистрации генерирует соответствующую запись. Если значения полей сравнения заданы, а системный вызов не указан, правило будет применяться ко всем системным вызовам. В одном правиле может быть задано несколько системных вызовов - это положительно сказывается на производительности, поскольку заменяет обработку нескольких правил;

Изм	Лист	№ докум	Подп	Дата

-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v]. Задать поле сравнения для правила. Атрибуты поля следующие: объект, операция, значение. Можно задать до 64 полей сравнения в одной команде. Каждое новое поле должно начинаться с -F. Служба регистрации событий будет генерировать запись, если произошло совпадение по всем полями сравнения. Допустимо использование одного из следующих 8 операторов: равно, не равно, меньше, больше, меньше либо равно, больше либо равно, битовая маска (n&v) и битовая проверка (n&=v). Битовая проверка выполняет операцию 'and' над значениями и проверяет, равны ли они. Битовая маска просто выполняет операцию 'and'. Поля, оперирующие с идентификатором пользователя, могут также работать с именем пользователя - программа автоматически получит идентификатор пользователя из его имени;

-A list,action. Добавить правило в начало списка list с действием action;

-C [f=f | f!=f]. Сравнить значения полей между собой. Формат задания сравнения: поле, оператор, поле. Можно в одной команде сравнивать несколько пар полей одновременно, перед каждой новой парой записывается опция -C. Опция снабжена двумя операторами: "=" и "!=". Доступные для сравнения поля;

-w путь. Добавить точку наблюдения за файловым объектом, находящимся по указанному пути;

-W путь. Удалить точку наблюдения за файловым объектом, находящимся по указанному пути.

Например, добавить правило аудита, осуществляющее наблюдение за доступом к файлу /etc/profile, можно с помощью команды:

```
auditctl -w /etc/profile -p rw -k profile
```

## 4.2 Утилита **autrace**

Утилита **autrace** позволяет добавлять правила регистрации событий безопасности для того, чтобы следить за использованием системных вызовов в указанном процессе. Она поддерживает опцию (-r), с помощью которой можно ограничить сбор информации о системных вызовах только теми, которые необходимы для анализа использования ресурсов.

Например, получение администратором информации из журналов аудита с помощью утилиты **autrace** может выглядеть следующим образом:

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost ~]# atrace /bin/date
Waiting to execute: /bin/date
Пн apr 9 22:56:19 MSK 2018
Cleaning up...
Trace complete. You can locate the records with 'ausearch -i -p 12438'
[root@localhost ~]#
```

Снимок экрана 48 – Получение информации из журнала аудита

### 4.3 Утилита ausearch

Утилита ausearch используется для поиска данных регистрации событий безопасности по различным критериям. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- a, --event audit-event-id. Искать события с заданным идентификатором события;
- c, --comm comm-name. Искать события с заданным именем исполняемого файла;
- f, --file file-name. Искать события с заданным именем файла;
- tm, --terminal terminal. Искать события с заданным терминалом;
- x, --executable executable. Искать события с заданной исполняемой программой;
- session Login-Session-ID. Искать события с заданным идентификатором сессии;
- ua, --uid-all all-user-id. Искать события, у которых любой из идентификаторов пользователя совпадает с заданным идентификатором пользователя;
- ue, --uid-effective effective-user-id. Искать события с заданным эффективным идентификатором пользователя;
- ui, --uid user-id. Искать события с заданным идентификатором пользователя;
- ga, --gid-all all-group-id. Искать события с заданным эффективным или обычным идентификатором группы;
- ge, --gid-effective effective-group-id. Искать события с заданным эффективным идентификатором группы или именем группы;
- gi, --gid group-id. Искать события с заданным идентификатором группы или именем группы;
- hn, --host host-name. Искать события с заданным именем узла. Имя узла может быть именем узла, полным доменным именем или цифровым сетевым адресом;
- k, --key key-string. Искать события с заданным ключевым словом;
- p, --pid process-id. Искать события с заданным идентификатором процесса;
- pp, --ppid parent-process-id. Искать события с заданным идентификатором родительского процесса;

Изм	Лист	№ докум	Подп	Дата

- sc, --success syscall-name-or-value. Искать события с заданным системным вызовом;
- o, --object SE-Linux-context-string. Искать события с заданным объектом SELinux;
- se, --context SE-Linux-context-string. Искать события с заданным контекстом SELinux
- su, --subject SE-Linux-context-string. Искать события с заданным субъектом SELinux;
- sv, --success success-value. Искать события с заданным флагом успешного выполнения. Допустимые значения: yes (успешно) и no (неудачно);
- te, --end [end-date] [end-time]. Искать события, которые произошли раньше или во время указанной временной точки;
- ts, --start [start-date] [start-time]. Искать события, которые произошли после или во время указанной временной точки;
- w, --word. Совпадение с полным словом. Поддерживается для имени файла, имени узла, терминала и контекста SELinux;
- uu, --uuid uuid\_гостевой\_системы. Искать событие в гостевой ОС с заданным UUID;
- vm, --vm-name имя\_гостевой\_системы. Искать событие в гостевой ОС с заданным именем;
- just-one. Остановить поиск после появления первого события, удовлетворяющего критериям поиска;
- e, --exit exit-code-or-errno. Искать события по заданному системному вызову: коду возврата или номеру ошибки;
- input-logs. Использовать место нахождения файла логов, обозначенное в `/etc/audit/auditd.conf`;
- h, --help. Выдать справку об утилите.

Например, записи регистрации неудачных попыток аутентификации пользователей могут выглядеть так, как это представлено на Снимке экрана 49, а записи регистрации попыток пользователя *user* удалить журнальный файл `/var/log/secure` могут выглядеть так, как это представлено на Снимке экрана 50.

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost ~]# ausearch -m USER_AUTH -sv no
-----
time->Fri Apr 6 16:29:57 2018
type=USER_AUTH msg=audit(1523021397.237:415): pid=6171 uid=0 auid=1002 ses=1
subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantor=?
acct="user3" exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=?
res=failed'
-----
time->Fri Apr 6 16:30:20 2018
type=USER_AUTH msg=audit(1523021420.919:419): pid=6210 uid=0 auid=1002 ses=1
subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantor=?
acct="user3" exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=?
res=failed'
-----
time->Mon Apr 9 08:47:09 2018
type=USER_AUTH msg=audit(1523252829.104:198): pid=4473 uid=0 auid=1002 ses=1
subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantor=?
acct="user3" exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=?
res=failed'
-----
time->Mon Apr 9 10:54:05 2018
type=USER_AUTH msg=audit(1523260445.137:761): pid=10754 uid=0 auid=1002 ses=1
subj=system_u:system_r:xdm_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantor=?
acct="user3" exe="/usr/libexec/gdm-session-worker" hostname=? addr=? terminal=?
res=failed'
```

Снимке экрана 49 - регистрация неудачных попыток аутентификации

```
time->Fri Apr 13 13:09:35 2018
type=PATH msg=audit(1523614175.408:276): item=0 name="/var/log/secure" inode=4195083
dev=fd:00 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:var_log_t:s0
objtype=NORMAL
type=SYSCALL msg=audit(1523614175.408:276): arch=c000003e syscall=262 success=no
exit=-13 a0=ffffffffffff9c a1=6530c0 a2=7fffa25adf30 a3=100 items=1 ppid=5472
pid=5697 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000
sgid=1000 fsgid=1000 tty=tty4 ses=3 comm="rm" exe="/usr/bin/rm" subj=user_u:user_r:
user_t:s0 key=(null)
type=AVC msg=audit(1523614175.408:276): avc: denied { getattr } for pid=5697
comm="rm" path="/var/log/secure" dev="dm-0" ino=4195083 scontext=user_u:user_r:
user_t:s0 tcontext=system_u:object_r:var_log_t:s0 tclass=file
[root@localhost user3]#
```

Снимке экрана 50 - регистрация неудачных попыток удалить файл

#### 4.4 Утилита aureport

Утилита aureport позволяет генерировать отчеты по данным регистрации событий безопасности. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- u, --user. Отчет о пользователях;
- e, --event. Отчет о событиях;
- f, --file. Отчет о файлах;

Изм.	Лист	№ докум	Подп	Дата



-p, --pid. Отчет о процессах;

-s, --syscall. Отчеты о системных вызовах;

-t, --log. Отчет о временных рамках отчета;

-x, --executable. Отчет об исполняемых объектах;

-tm, --terminal. Отчет о терминалах;

-l, --login. Отчет о попытках входа в систему;

-au, --auth. Отчет о всех попытках аутентификации;

-c, --config. Отчет об изменениях конфигурации;

-m, --mods. Отчет об изменениях пользовательских учетных записей;

--tty. Отчёт о нажатиях пользователя на клавиатуре;

-ma, --mac. Отчет о событиях в системе мандатного управления доступом;

--success. Для обработки в отчетах выбирать только удачные события, по умолчанию показываются и удачные и неудачные события;

--failed. Для обработки в отчетах выбирать только неудачные события, по умолчанию показываются и удачные и неудачные события;

-te, --end [дата] [время]. Искать события, которые произошли раньше или во время указанной временной точки;

-ts, --start [дата] [время]. Искать события, которые произошли после или во время указанной временной точки;

--node имя\_узла. Выбрать события, связанные с узлом, имя которого указано после ключа. Можно указать несколько имён узлов, по умолчанию информация собирается со всех узлов;

--summary. Генерировать итоговый отчет, который дает информацию только о количестве элементов в том или ином отчете;

--input-logs. Использовать место нахождения файла логов, обозначенное в /etc/audit/auditd.conf.

Например, отчет о попытках аутентификации с 08:00 01.04.2018 до 20:50 10.04.2018 может выглядеть следующим образом:

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost ~]#
[root@localhost ~]# aureport -au --start 01/04/18 08:00 --end 10/04/18 20:50

Authentication Report
=====
# date time acct host term exe success event
=====
1. 06.04.2018 16:05:53 user3 ? ? /usr/libexec/gdm-session-worker yes 380
2. 06.04.2018 16:13:43 user3 ? ? /usr/libexec/gdm-session-worker yes 392
3. 06.04.2018 16:16:42 user3 ? ? /usr/libexec/gdm-session-worker yes 401
4. 06.04.2018 16:29:57 user3 ? ? /usr/libexec/gdm-session-worker no 415
5. 06.04.2018 16:30:20 user3 ? ? /usr/libexec/gdm-session-worker no 419
6. 06.04.2018 16:30:24 user3 ? ? /usr/libexec/gdm-session-worker yes 422
7. 09.04.2018 08:30:06 gdm ? ? /usr/libexec/gdm-session-worker yes 125
8. 09.04.2018 08:34:23 user3 ? ? /usr/libexec/gdm-session-worker yes 152
9. 09.04.2018 08:35:53 user3 ? ? /usr/libexec/gdm-session-worker yes 171
10. 09.04.2018 08:36:03 user3 ? ? /usr/lib/polkit-1/polkit-agent-helper-1 yes
```

Снимок экрана 51 - Отчет о попытках аутентификации

А отчет о попытках установления сеанса заблокированным пользователем может выглядеть следующим образом:

```
[root@localhost user]# aureport -au -ts recent

Authentication Report
=====
# date time acct host term exe success event
=====
1. 09.04.2018 14:30:39 user3 192.168.10.100 ssh /usr/sbin/sshd no 855
2. 09.04.2018 14:30:41 (unknown) 192.168.10.100 ssh /usr/sbin/sshd no 856
3. 09.04.2018 14:30:41 user3 192.168.10.100 ssh /usr/sbin/sshd no 857
4. 09.04.2018 14:30:43 (unknown) 192.168.10.100 ssh /usr/sbin/sshd no 858
5. 09.04.2018 14:30:44 user3 192.168.10.100 ssh /usr/sbin/sshd no 859
6. 09.04.2018 14:30:46 (unknown) 192.168.10.100 ssh /usr/sbin/sshd no 860
[root@localhost user]#
```

Снимок экрана 52 – Отчет о попытках входа в систему

#### 4.5 Конфигурационный файл /etc/audit/auditd.conf

Конфигурационный файл /etc/audit/auditd.conf содержит параметры настройки средств регистрации событий безопасности (см. Снимки экрана 53 и 54), в том числе:

**log\_file.** Полное имя файла, в котором будут храниться данные регистрации событий безопасности;

**log\_group.** Группа, являющаяся владельцем файла регистрации;

**log\_format.** Формат хранения данных регистрации, возможные значения: raw (данные записываются в том виде, в каком они были получены от ядра операционной системы) и nolog (запись данных отключается);

**priority\_boost.** Приоритет выполнения службы регистрации;

Изм	Лист	№ докум	Подп	Дата

`flush`. Режим работы службы регистрации, возможные значения: `none` (не использовать какие-либо политики записи, т.е. дополнительные действия), `incremental` (запись с периодичностью, определенной параметром `freq`), `data` (запись данных в синхронном режиме), `sync` (запись в синхронном режиме и данных и метаданных файла);

`freq`. Максимальное число регистрационных записей, которые могут храниться в буфере перед записью буферизованных данных на диск, используется только когда параметр `flush` имеет значение `incremental`;

`num_logs`. Максимальное число файлов регистрации на диске, используется только когда параметр `max_log_file_action` имеет значение `rotate`, значение параметра не должно превышать 99;

`disp_qos`. Режим передачи данных между службой регистрации и диспетчером, возможные значения: `lossy` (блокирование запрещено, т.е. служба регистрации может не передавать диспетчеру некоторые данные о событиях, если очередь данных о событиях полна, при этом данные регистрации будут записаны на диск, если только значение параметра `log_format` не равно `nolog`), `lossless` (блокирование разрешено, т.е. запись данных регистрации о событиях на диск будет остановлена, пока не освободится место в очереди);

`dispatcher`. Место расположения исполняемого файла программы диспетчера;

`name_format`. Порядок разрешения имен хостов, возможные значения: `none` (имя не используется), `hostname` (имя, возвращенное через запрос `gethostname`), `fqd` (полное имя хоста, возвращенное через DNS запрос) `numeric` (ip адрес), `user` (строка, определенная в параметре `name`);

`max_log_file`. Максимальный размер файла регистрации в мегабайтах, по достижению которого будет выполнено действие, определенное параметром `max_log_file_action`, возможные действия: `ignore` (ничего не делать), `syslog` (отправить предупреждение в `syslog`), `suspend` (остановить запись данных регистрации событий на диск), `rotate` (произвести ротацию файлов регистрации в соответствии с параметром `num_logs`), `keep_logs` (осуществить ротацию, при этом не удалять старые файлы);

`space_left`. Величина в мегабайтах, определяющая размер оставшегося дискового пространства, при достижении которого будет выполнено действие `space_left_action`, возможные действия: `ignore` (ничего не делать), `syslog` (отправить предупреждение в `syslog`), `email` (отправить письмо аккаунту, определенному в `action_mail_acct`), `exec` (выполнить

Изм	Лист	№ докум	Подп	Дата

скрипт), suspend (остановить запись на диск и перевести систему в single mode), halt (выключить систему);

admin\_space\_left. Величина в мегабайтах оставшегося свободного пространства на диске для предупреждения администратора, что надо добавить/очистить свободное пространство. Величина должна быть меньше чем space\_left. Действия, которые можно определить в admin\_space\_left\_action, аналогичны space\_left\_action;

disk\_full\_action. Действия, выполняемые при заполнении всего дискового пространства, аналогичны space\_left\_action;

disk\_error\_action. Действия, выполняемые при возникновении дисковой ошибки, аналогичны space\_left\_action.

```
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = root
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = ROTATE
space_left = 75
space_left_action = SYSLOG
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port =
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
:█
```

Снимок экрана 53 – Конфигурационный файл /etc/audit/auditd.conf (1)

Изм	Лист	№ докум	Подп	Дата

```
#  
  
local_events = yes  
write_logs = yes  
log_file = /var/log/audit/audit.log  
log_group = root  
log_format = RAW  
flush = INCREMENTAL_ASYNC  
freq = 50  
max_log_file = 8  
num_logs = 5  
priority_boost = 4  
disp_qos = lossy  
dispatcher = /sbin/audispd  
name_format = NONE  
##name = mydomain  
max_log_file_action = ROTATE  
space_left = 75  
space_left_action = SYSLOG  
action_mail_acct = root  
admin_space_left = 50  
admin_space_left_action = SUSPEND  
disk_full_action = SUSPEND  
disk_error_action = SUSPEND  
use_libwrap = yes  
##tcp_listen_port =  
tcp_listen_queue = 5  
tcp_max_per_addr = 1  
##tcp_client_ports = 1024-65535  
tcp_client_max_idle = 0  
enable_krb5 = no  
krb5_principal = auditd  
##krb5_key_file = /etc/audit/audit.key  
distribute_network = no  
(END)
```

Снимок экрана 54 – Конфигурационный файл /etc/audit/auditd.conf (2)

Изм	Лист	№ докум	Подп	Дата

## 5 ОГРАНИЧЕНИЕ ПРОГРАММНОЙ СРЕДЫ

Средства ограничения программной среды предоставляют возможности установки программного обеспечения доверенным образом; применения типовых наборов различных программных конфигураций; управления запуском программного обеспечения, в том числе определения запускаемых программ, настройки параметров запуска и контроля за их запуском; реагирования на попытки запуска, произведенные в нарушение установленных правил, а также другие возможности.

### 5.1 Утилита `chkconfig`

Утилита `chkconfig` позволяет включать программы в так называемую автозагрузку с целью их автоматического запуска при старте операционной системы. Она поддерживает следующий набор опций:

`--level levels`. Определяет уровни, на которых соответствующая программа должна выполняться. Уровни указываются на месте параметра `levels` в качестве строки целочисленных значений в диапазоне от 0 до 6. Так, например, при передаче опции `--level 35` утилите будет передано указание на уровни 3 и 5 соответственно;

`--no-redirect`. Если утилита запущена в системе, использующей утилиту `systemd` в качестве системы инициализации, то `chkconfig` будет перенаправлять команды в `systemd`, если у данной службы существует соответствующий файл, предназначенный для таких обращений. Данная опция отключает процесс перенаправления утилите `systemd` и обеспечивает работу только с символьными ссылками в директориях `/etc/rc[0-6].d`;

`--add name`. Добавляет новую службу для управления утилитой `chkconfig`. Имя службы указывается на месте параметра `name`;

`--del name`. Удаляет службу, имя которой указывается на месте параметра `name`, из под управления утилитой `chkconfig`. Также из директорий `/etc/rc[0-6].d` удаляются любые символьные ссылки, указывающие на удаляемую службу;

`--override name`. Производит переопределение настроек службы, имя которой указывается на месте параметра `name`, вместо базовых настроек;

`--list name`. Выводит все службы, доступные для `chkconfig`, а также показывает их статус на каждом уровне (вкл/выкл). Если опции передать аргументом имя некоторой

Изм	Лист	№ докум	Подп	Дата

службы, которое указывается на месте параметра name, то будет выведена информация только об указанной службе.

## 5.2 Утилита `systemctl`

Утилита `systemctl` позволяет управлять системными службами. Она поддерживает следующий набор опций:

`-t, --type`. Указывает на тип так называемого юнита (службы, сокета, устройства и т.п.), может быть в виде списка наименований типов, разделенных запятой, если требуется указать более, чем на один тип;

`-a, --all`. При выведении списка юнитов вывести абсолютно все загруженные юниты, вне зависимости от их статуса, включая те из них, которые являются неактивными;

`start` [имя сервиса]. Запускает работу сервиса с указанным именем;

`stop` [имя сервиса]. Останавливает работу сервиса с указанным именем;

`reload` [имя сервиса]. Перезагружает конфигурацию сервиса с указанным именем;

`restart` [имя сервиса]. Перезапускает сервис с указанным именем;

`try-restart` [имя сервиса]. Перезапускает сервис с указанным именем, если данный сервис уже работает на момент запуска утилиты;

`reload-or-restart` [имя сервиса]. Перезагрузить конфигурацию сервиса с указанным именем, если сервис поддерживает такую команду, или выполнить перезапуск службы. Если на момент запуска утилиты указанная служба не была запущена, то она запустится после успешного выполнения команды;

`reload-or-try-restart` [имя сервиса]. Перезагрузить конфигурацию сервиса с указанным именем, если сервис поддерживает такую команду, или выполнить перезапуск службы. Если на момент запуска утилиты указанная служба не была запущена, то указанная команда не произведет никаких действий;

`kill` [имя сервиса]. Осуществить принудительную остановку работы службы с указанным именем;

`is-active` [имя сервиса]. Осуществляет проверку, активна ли на момент запуска утилиты служба с указанным именем. Если служба активна, или хотя бы одна из служб, переданных в качестве аргумента данной команде, активна (в случае, если были переданы наименования более, чем одной службы), выведется нулевое значение, в противном случае – ненулевое;

Изм	Лист	№ докум	Подп	Дата

is-failed [имя сервиса]. Проверяет, были ли проблемы при запуске указанной службы или служб. Если хотя бы у одной из служб возникали проблемы, будет выведено нулевое значение;

enable [имя сервиса]. Добавляет указанный сервис (или их множество) в автозапуск;

disable [имя сервиса]. Убирает указанный сервис (или их множество) из автозапуска;

is-enabled [имя сервиса]. Проверяет, находится ли указанная служба (или службы, в случае, если в качестве аргумента был передан список наименований) в автозапуске. Если хотя бы одна из указанных служб находится в автозапуске, будет выведено нулевое значение;

--version. Вывести информацию о версии утилиты;

-h, --help. Вывести справочную информацию об утилите.

Например, проверка статуса сервера печати может выглядеть следующим образом:

```
[root@localhost ~]# systemctl status cups
● cups.service - CUPS Printing Service
   Loaded: loaded (/usr/lib/systemd/system/cups.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
```

Снимок экрана 55 - Проверка статуса сервера печати

А разрешение автоматического запуска сервера печати CUPS при загрузке системы может выглядеть следующим образом:

```
[root@localhost ~]# systemctl enable cups
Created symlink from /etc/systemd/system/multi-user.target.wants/cups.service to /usr/lib/systemd/system/cups.service.
Created symlink from /etc/systemd/system/printer.target.wants/cups.service to /usr/lib/systemd/system/cups.service.
Created symlink from /etc/systemd/system/sockets.target.wants/cups.socket to /usr/lib/systemd/system/cups.socket.
Created symlink from /etc/systemd/system/multi-user.target.wants/cups.path to /usr/lib/systemd/system/cups.path.
[root@localhost ~]# reboot
```

Снимок экрана 56 – Разрешение автоматического запуска сервера печати

### 5.3 Утилита crontab

Утилита crontab позволяет настраивать запуск программ по расписанию. Она поддерживает следующий набор опций:

-u. Указывает пользователя, чье расписание должно редактироваться;

-l. Вывод текущего файла расписания;

-r. Удаление текущего файла расписания;

Изм	Лист	№ докум	Подп	Дата



-е. Редактирование файла расписания.

Таблица расписания состоит из шести колонок, разделяемых пробелами или табуляторами. Первые пять колонок задают время выполнения (*минута, час, день, месяц, день недели*), в них может находиться число, список чисел, разделённых запятыми, диапазон чисел, разделённых дефисом, символы `*` или `/`. После полей времени указывается пользователь, от которого запускается программа. Все остальные символы в строке интерпретируются как выполняемая программа с её параметрами.

Например установим с помощью утилиты `crontab` ограничения на доступ к системе по времени, с 10:28 до 10:30 (см. Снимок экрана 57). Команда `"passwd -l user2"` блокирует возможность авторизации, дописывая символ восклицательного знака к строке пароля в файле `/etc/shadow`. Команда `"passwd -u user2"` производит обратную операцию, снимая тем самым блокировку. После чего выполним команду `"service crond restart"`.

```
[root@localhost user]# crontab -e
crontab: installing new crontab
[root@localhost user]#
[root@localhost user]# service crond restart
Redirecting to /bin/systemctl restart crond.service
[root@localhost user]#
[root@localhost user]# crontab -l
28 10 * * * /usr/bin/passwd -l user2
30 10 * * * /usr/bin/passwd -u user2
[root@localhost user]#
```

Снимок экрана 57 - Ограничение входа в систему по времени

## 5.4 Утилита `rpm`

Утилита `rpm` позволяет управлять так называемыми программными пакетами, т.е. управлять их установкой, обновлением, проверкой и удалением. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

`-i, --install`. Установка нового пакета;

`-u, --upgrade`. Установка или обновление уже установленного пакета до новой версии.

При этом, после установки пакета все другие версии удаляются;

`-f, --freshen`. Обновление пакета, но только, если предыдущая версия уже установлена;

`--nodeps`. Не выполнять проверку зависимостей перед установкой или обновлением пакета;

`--nosuggest`. Не предлагать пакет(ы) для разрешения отсутствующих зависимостей;

Изм	Лист	№ докум	Подп	Дата

--noorder. Не выполнять переупорядочивание пакетов для установки. Список пакетов обычно переупорядочивается для удовлетворения зависимостей;

--oldpackage. Разрешает обновить или заменить пакет более старой версией;

--replacefiles. Установить пакеты, даже если они заменяют файлы от других установленных пакетов;

--replacesrcks. Установить пакеты, даже если они уже установлены в системе;

--includedocs. Устанавливать файлы с документацией;

--excludedocs. Не устанавливать документацию;

-e, --erase. Удалить заданный пакет;

--allmatches. Удалить все версии пакета;

--nodeps. Не проверять зависимости перед удалением пакетов;

--test. Выполнить только проверку установки пакета;

-q, --query. Вывести информацию о пакете;

-a, --all. Выполняет запрос ко всем установленным пакетам;

--changelog. Вывести информацию об изменениях в пакете;

-l, --list. Вывести список файлов в пакете;

--provides. Вывести функциональность, предоставляемую пакетом;

-R, --requires. Вывести пакеты, от которых зависит этот пакет;

-v, --verify. Выполнить проверку метаданных пакета и его контрольной суммы;

--version. Вывести номер версии утилиты;

--help. Вывести справку об использовании утилиты.

### 5.5 Утилита yum

Утилита yum используется для установки последней версии пакета или группы пакетов с учетом существующих зависимостей. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

install. Используется для установки последней версии пакета или группы пакетов с учетом существующих зависимостей;

reinstall. Используется для переустановки пакета с идентичной версией;

update. Используется для обновления. Если без указания пакетов, то будут обновлены все установленные пакеты. Если указан один или более пакетов, то будут обновлены только перечисленные пакеты. При обновлении учитываются зависимости;

Изм	Лист	№ докум	Подп	Дата

downgrade. Пытаться понизить пакет с версии, установленной в данный момент, до предыдущей самой высокой версии или указанной версии;

upgrade. Производится полное обновление системы. Удобно для смены версии дистрибутива, так как при этом учитывается замена устаревших пакетов другими, более новыми;

remove. Используется для удаления указанных пакетов из системы, а также для удаления пакетов, зависящих от удаляемых пакетов. Также эту функцию можно вызвать командой erase, это синонимы;

list. Используется для вывода различной информации о доступных пакетах;

search. Используется для поиска пакетов;

provides. Используется, чтобы выяснить, какой пакет предоставляет тот или иной файл;

info. Используется для вывода описаний и общей информации о доступных пакетах;

clean. Используется для удаления различных данных, накапливающихся со временем в кэше утилиты;

deplist. Вывести зависимости пакета;

-x, --exclude. Исключить пакет из обновлений;

-v, --verbose. Запустить с большим количеством отладочной информации;

-d, --debuglevel. Устанавливает уровень отладки;

-h, --help. Вывести справку и выйти.

Изм	Лист	№ докум	Подп	Дата

## 6 СТИРАНИЕ ДАННЫХ

Средства стирания данных предоставляют возможности безвозвратного удаления ставших ненужными данных и обеспечения недоступности остаточной информации путем многократной перезаписи использованных мест памяти специальными последовательностями.

### 6.1 Утилита **shred**

Утилита **shred** позволяет заполнять случайными числами место, занятое файлами. Она поддерживает следующий набор опций:

-f, --force. Изменить права для разрешения записи, если это необходимо;

-n, --iterations=N. Перезаписать файл N раз вместо 3-х по умолчанию;

--random-source=FILE. Перезаписать файл случайными данными, взятыми из файла с именем FILE;

-s, --size=N. Перезаписать только N байт, можно использовать суффиксы К, М, G для указания размерности: килобайт, мегабайт, гигабайт;

-u, --remove. Обрезать и удалить файл после перезаписи. По умолчанию файлы не удаляются;

-v, --verbose. Показывать ход выполнения;

-x, --exact. Не округлять размер файла до следующего целого блока;

-z, --zero. На последней итерации перезаписать файл нулями;

--version. Показать версию утилиты и выйти;

--help. Показать справку и выйти.

Например, для заполнения места, занятого файлом *filename* с последующим удалением файла необходимо выполнить команду:

```
shred -u -z filename
```

### 6.2 Утилита **sfill**

Утилита **sfill** позволяет стирать данные в свободном пространстве раздела, в котором находится заданная директория. Стирание производится в четыре шага: однократная перезапись числами 255 (0xFF), пятикратная перезапись случайными числами,

Изм	Лист	№ докум	Подп	Дата

двадцатисемикратная перезапись специальными числами и еще один раз пятикратная перезапись случайными числами. Утилита поддерживает следующий набор опций:

-f. Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами;

-i. Очистка свободного пространства только индексного дескриптора, но не свободного пространства жесткого диска;

-I. Очистка свободного пространства только жесткого диска, не затрагивая свободное пространство индексного дескриптора;

-l. Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды (например, `sdmем -l -l`);

-v. Работа будет сопровождаться выводом динамической строки, указывающей прогресс ее выполнения;

-z. На четвертом шаге вместо перезаписи случайными числами выполнять перезапись нулями.

Например, очистка свободного пространства может выглядеть следующим образом:

```
[root@localhost ~]# sfill -vz /mnt/
Using /dev/urandom for random input.
Wipe mode is secure (38 special passes)
Wiping now ...
Creating /mnt/00000000.000 ... ***** Wiping inodes ...
Done ... Finished
[root@localhost ~]#
```

Снимок экрана 58 – Очистка свободного пространства

### 6.3 Утилита `sswap`

Утилита `sswap` позволяет стирать данные в так называемых разделах подкачки. Алгоритм стирания данных абсолютно такой же, как и у утилиты `sfill`. Поддерживается похожий набор опций, в том числе:

-f. Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами;

-l. Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды;

Изм	Лист	№ докум	Подп	Дата

-v. Работа будет сопровождаться выводом динамической строки, указывающей прогресс ее выполнения;

-z. На четвертом шаге вместо перезаписи случайными числами выполнять перезапись нулями.

#### **6.4 Утилита `sdmem`**

Утилита `sdmem` позволяет стирать данные в оперативной памяти. Алгоритм стирания данных почти такой же, как и у утилиты `sfill`, но с тем отличием, что на первом шаге однократная перезапись производится числами 0 (0x00). Поддерживается похожий набор опций, в том числе:

-f. Выполнение более быстрым образом за счет пропуска второго и четвертого шагов перезаписи случайными числами;

-l. Выполнение более быстрым образом за счет пропуска третьего и четвертого шагов или путем выполнения только одного шага перезаписи данных нулевыми значениями, если эту опцию задать дважды;

-v. Работа будет сопровождаться выводом динамической строки, указывающей прогресс ее выполнения.

Изм	Лист	№ докум	Подп	Дата

## 7 КОНТРОЛЬ ЦЕЛОСТНОСТИ

Средства контроля целостности предоставляют возможности контроля целостности обрабатываемых данных и используемого программного обеспечения.

### 7.1 Утилита md5sum

Утилита md5sum позволяет вычислять контрольные суммы файлов по алгоритму MD5 и осуществлять их сверку с другими контрольными суммами, хранящимися в файле. Она поддерживает следующий набор опций:

- b, --binary. Позволяет считывать данные из файлов в двоичном режиме;
- t, --text . Позволяет считывать данные из файлов в текстовом режиме;
- c, --check. Позволяет осуществить сверку рассчитанного значения контрольной суммы с некоторым другим значением контрольной суммы, хранящимся в файле, имя которого должно быть передано утилите в качестве аргумента;
- tag. Выводить рассчитанную контрольную сумму в формате BSD;
- quiet. При сверке контрольных сумм позволяет не выводить сообщение «ОК» для каждого успешного случая сверки контрольных сумм;
- status. При сверке контрольных сумм позволяет в конце работы утилиты не выводить ничего, кроме кода сверки контрольных сумм;
- strict. При сверке контрольных сумм выводить ненулевое значение для неправильно отформатированных строк контрольной суммы;
- w. При сверке контрольных сумм выводить предупреждения о неправильно отформатированных строках контрольной суммы;
- version. Выводит информацию о версии утилиты;
- help. Выводит справку для утилиты.

Например, подсчет контрольной суммы файла с журналом аудита может выглядеть следующим образом:

```
[root@localhost ~]# md5sum /var/log/audit/audit.log
7125d47d351f46de50e73aaf8df016f5 /var/log/audit/audit.log
[root@localhost ~]#
```

Снимок экрана 59 - Подсчет контрольной суммы журнала аудита

Изм	Лист	№ докум	Подп	Дата

## 7.2 Утилита **aide**

Утилита **aide** предоставляет возможности проверки целостности данных. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-i, --init. Инициализирует так называемую базу данных хранения состояний файлов. Созданная после инициализации база данных должна быть размещена в таком месте, из которого при осуществлении последующей проверки данные могли бы быть считаны. В противном случае, при попытке осуществления проверки будет выведена информация об ошибке считывания;

-C, --check. Проверяет базу данных состояний файлов на наличие несоответствий, для чего необходимо иметь инициализированную базу данных. Эта опция выполняется по умолчанию, если не указать никакой другой опции;

-u, --update. Проверяет базу данных и обновляет ее, при этом входные и выходные базы данных должны быть разными;

-E, --compare. Сравнивает две базы данных, которые должны быть определены в конфигурационном файле;

-D, --config-check. Осуществляет считывание данных из конфигурационного файла, уведомляя обо всех обнаруженных ошибках;

-c, --config=configfile. Позволяет считывать конфигурацию из указанного файла вместо используемого по умолчанию конфигурационного файла «./aide.conf»;

-B, --before="configparameters". Позволяет обрабатывать указанные конфигурационные параметры до считывания данных из конфигурационного файла;

-A, --after="configparameters". Позволяет обрабатывать указанные конфигурационные параметры после считывания данных из конфигурационного файла;

-Vverbosity\_level, --verbose=verbosity\_level. Определяет детальность обработки данных. На месте параметра `verbosity_level` может находиться целочисленное значение в диапазоне от 0 до 255. По умолчанию значение данного параметра равно 5. Если вызвать данную опцию, но не присвоить целочисленное значение параметру `verbosity_level`, то ему автоматически будет присвоено значение, равное 20. Этот параметр переопределяет значение, установленное в конфигурационном файле;

-r reporter, --report=reporter. Определяет место (URL), в которое утилита должна направлять свои результаты работы.

Изм	Лист	№ докум	Подп	Дата



Например, проверим систему, сравнив aide.db и текущее состояние системы, без обновления aide.db.new:

```
[root@localhost user3]# aide -C
AIDE, version 0.15.1
### All files match AIDE database. Looks okay!
[root@localhost user3]#
```

Снимок экрана 60 – Проверка системы

Если произошло изменение файлов системы, то будет получено соответствующее уведомление:

```
[root@localhost aide]# aide -C
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2018-03-28 09:12:21

Summary:
  Total number of files:      264416
  Added files:                1
  Removed files:              0
  Changed files:              3

-----
Added files:
-----
added: /root/.xauthyBkzld

-----
Changed files:
-----
changed: /etc/cups/subscriptions.conf
changed: /etc/cups/subscriptions.conf.0
changed: /root/.cache/abrt/lastnotification

-----
Detailed information about changes:
-----

File: /etc/cups/subscriptions.conf
SHA256  : m6TGBQ90ZSbJCmv496H6LPHzGg9lsI1l , mRnhVE4l55upDLx8q2LeJNa6z8t7i1t4

File: /etc/cups/subscriptions.conf.0
SHA256  : vumWxfS6Lw16IaIDBd9+DfNh649t8D0i , 539PzGivsc2Xy9xHt0yBjmRSqsZHR+Co

File: /root/.cache/abrt/lastnotification
SELinux : system_u:object_r:admin_home_t:s0, unconfined_u:object_r:admin_home_t:s0
[root@localhost aide]# █
```

Снимок экрана 61 – Уведомление об изменениях

Изм	Лист	№ докум	Подп	Дата

## 8 ОБЕСПЕЧЕНИЕ НАДЕЖНОГО ФУНКЦИОНИРОВАНИЯ

Средства обеспечения надежного функционирования предоставляют возможности резервного копирования и восстановления данных и программного обеспечения при сбоях и отказах, а также возможности функционирования отдельных экземпляров системы на нескольких технических средствах в отказоустойчивом режиме, обеспечивающем доступность сервисов и данных при выходе из строя одного из технических средств или при исчерпании вычислительных ресурсов.

### 8.1 Утилита tar

Утилита tar позволяет архивировать файлы и директории со всеми их поддиректориями и файлами, а затем восстанавливать их из архива, т.е. является удобным средством для создания резервных копий. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- c, --create. Создать новый архив;
- r, --append. Присоединить файлы к концу архива;
- delete. Удалить файл из архива;
- t, --list. Вывести список содержимого архива;
- A, --catenate, --concatenate. Присоединить существующий архив к другому архиву;
- x, --extract, -get. Извлечь файлы из архива;
- u, --update. Добавить в архив более новые версии файлов;
- C, --directory=DIR. Сменить директорию перед выполнением операции на DIR;
- f, --file=ARCHIVE. Вывести результат в архивный файл или в устройство ARCHIVE;
- d, --diff. Осуществить проверку на наличие различий между архивом и некоторой файловой системой;
- v, --verbose. Выводить подробную информацию о процессе выполнения команды.

В следующем примере директория *mydir* и все ее поддиректории сначала сохраняются в файле *myarch.tar*:

```
tar cf myarch.tar mydir
```

а затем извлекаются из архива:

```
tar xf myarch.tar
```

Изм	Лист	№ докум	Подп	Дата

А этот скрипт организует хранение четырех последних резервных копий директории /var/www в директории /opt/backup/www-backup. Первая версия будет всегда иметь номер 0, последняя – номер 3. При создании новых версий старые будут удаляться. Сами резервные копии хранятся в сжатом архиватором виде.

```
#!/bin/bash
cd /opt/backup/www-backup
rm www-dump-3.tar.gz
cp www-dump-2.tar.gz www-dump-3.tar.gz
cp www-dump-1.tar.gz www-dump-2.tar.gz
cp www-dump-0.tar.gz www-dump-1.tar.gz
tar --selinux --acls --xattrs -czf www-dump-0.tar.gz /var/www
```

Снимок экрана 62 – Создание резервных копий

## 8.2 Утилита `сrio`

Утилита `сrio` используется для создания архивов и извлечения файлов из них, а также для копирования файлов в целях их переноса из текущей директории в другую. Поддерживает множество различных архивных форматов. При извлечении файлов из архива, утилита автоматически распознает, каким типом обладает архив, с которым она взаимодействует.

Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

-o, --create. Копировать файлы в архив;

-A, --append. Добавить файлы в архив, может быть использована только в связке с опцией -o;

-i, --extract. Копирует файлы из архива или выводит список содержимого некоторого архива;

-p, --pass-through. Копирует файлы из одной файловой структуры в другую, комбинируя при этом режимы работы, использующиеся при передаче опций -i и -o, но не используя при этом архивы;

-a, --reset-access-time. Сбрасывает времена обращения к входным файлам после их копирования, так что при использовании данной опции будет нельзя распознать, что файлы были скопированы.

В следующем примере сначала флеш-носитель монтируется как устройство `/mnt`:

```
mount /dev/sdb4 /mnt
```

Изм	Лист	№ докум	Подп	Дата

Затем создается и записывается на флеш-носитель резервная копия директории *lib*:

```
find /lib/ | cpio -o > /mnt/2/backup.cpio
```

Для того, чтобы восстановить все файлы в директорию *lib* из созданной ранее архивной копии, необходимо выполнить:

```
cpio -ivmd /lib/\* < /mnt/2/backup.cpio
```

### 8.3 Утилиты amanda

Система утилит amanda обладает возможностью резервного копирования данных, хранящихся на множестве компьютеров в вычислительной сети. Она реализует клиент-серверную модель и использует следующие утилиты:

клиентская утилита amandad, взаимодействующая с сервером системы. Во время своего выполнения вызывает другие утилиты: selfcheck (проверка конфигурации клиента), sendsize (оценка объема резервной копии), sendbackup (выполнение операции резервного копирования), amcheck (проверка конфигурации системы);

серверная утилита amdump, инициирующая все операции резервного копирования. Во время своего выполнения использует другие утилиты и контролирует их выполнение: planner (определение того, что надо копировать), driver (интерфейс к внешнему устройству), dumper (связывается с клиентским процессом amandad), taper (запись данных на внешнее устройство), amreport (подготовка сообщения о выполненном копировании);

административные утилиты: amcheck (проверка системы, чтобы убедиться, что система готова к работе), amlabel (записать метку на сменный носитель перед использованием в системе), amcleanup (очистить систему после не плановой перезагрузки сервера или после не планового завершения операции резервного копирования), amflush (переписать данные из дискового кэша на внешний носитель) amadmin (выполнение большого количества различных административных операций);

утилиты восстановления данных: amrestore (восстановление данных с носителей, на которых записаны резервные копии, выполненные системой), amrecover (программа для интерактивного восстановления данных с резервных копий).

Изм	Лист	№ докум	Подп	Дата

#### 8.4 Утилита mdadm

Утилита mdadm позволяет создавать так называемые дисковые RAID массивы с использованием технологии распределения данных по нескольким дискам с целью достижения избыточности, отказоустойчивости, сокращения задержек и/или увеличения скорости чтения и записи, а также для улучшения возможностей восстановления данных в случае отказа. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- A, --assemble. Режим сборки ранее созданного массива и его активации;
- B, --build. Режим сборки массива без суперблоков;
- C, --create. Режим сборки нового массива;
- F, --follow, --monitor. Режим слежения за состоянием устройств;
- G, --grow. Режим расширения или уменьшения размера массива;
- N, --name. Устанавливает имя массива;
- n, --raid-devices. Указывает количество активных устройств в массиве;
- x, --space-device. Указывает количество запасных устройств в массиве;
- z, --size. Указывает объем пространства, используемого для каждого диска;
- l, --level. Устанавливает уровень массива;
- c, --config. Указывает файл конфигурации, по умолчанию /etc/mdadm.conf;
- f, --fail. Помечает перечисленные устройства, как неисправные;
- S, --stop. Деактивирует массив и освобождает все ресурсы;
- V --version. Вывести информацию о версии утилиты;
- h, --help. Вывести справку об утилите.

Рассмотрим пример объединения нескольких внешних устройств энергонезависимой памяти в RAID-массив, обеспечивающий доступность информации, в случае выхода из строя одного из них. Установим в компьютер два usb-накопителя и на каждом из них создадим два раздела размером 500Мб:

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost /]# fdisk /dev/sdd
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Команда (m для справки): o
Building a new DOS disklabel with disk identifier 0x582d0068.

Команда (m для справки): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p):
Using default response p
Номер раздела (1-4, default 1):
Первый sector (2048-7866367, по умолчанию 2048):
Используется значение по умолчанию 2048
Last sector, +sectors or +size{K,M,G} (2048-7866367, по умолчанию 7866367): +500M
Partition 1 of type Linux and of size 500 MiB is set

Команда (m для справки): w
Таблица разделов была изменена!

Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
[root@localhost /]#
```

Снимок экрана 63 - Создание раздела на первом usb-накопителе

```
[root@localhost /]# fdisk /dev/sde
Welcome to fdisk (util-linux 2.23.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Команда (m для справки): o
Building a new DOS disklabel with disk identifier 0xfd0ffa4.

Команда (m для справки): n
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Номер раздела (1-4, default 1):
Первый sector (2048-30218841, по умолчанию 2048):
Используется значение по умолчанию 2048
Last sector, +sectors or +size{K,M,G} (2048-30218841, по умолчанию 30218841): +500M
Partition 1 of type Linux and of size 500 MiB is set

Команда (m для справки): w
Таблица разделов была изменена!

Вызывается ioctl() для перечитывания таблицы разделов.
Синхронизируются диски.
[root@localhost /]#
```

Снимок экрана 64 - Создание раздела на втором usb-накопителе

Используем созданные разделы для сборки RAID массива (зеркало), как показано ниже:

Изм	Лист	№ докум	Подп	Дата

```
[root@localhost /]# mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sdd1 /dev/sde1
mdadm: Note: this array has metadata at the start and
may not be suitable as a boot device. If you plan to
store '/boot' on this device please ensure that
your boot-loader understands md/v1.x metadata, or use
--metadata=0.90
Continue creating array?
Continue creating array? (y/n) y
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md1 started.
[root@localhost /]#
```

Снимок экрана 65 - Сборка RAID массива

А теперь выведем информацию о собранном RAID массиве:

```
[root@localhost /]# mdadm -D /dev/md1
/dev/md1:
  Version : 1.2
  Creation Time : Mon Feb 12 16:02:53 2018
  Raid Level : raid1
  Array Size : 511680 (499.69 MiB 523.96 MB)
  Used Dev Size : 511680 (499.69 MiB 523.96 MB)
  Raid Devices : 2
  Total Devices : 2
  Persistence : Superblock is persistent

  Update Time : Mon Feb 12 16:04:51 2018
  State : clean
  Active Devices : 2
  Working Devices : 2
  Failed Devices : 0
  Spare Devices : 0

  Name : localhost.localdomain:1 (local to host localhost.localdomain)
  UUID : 2c283ef5:f8a1ebe6:42a58684:59bda77b
  Events : 19

   Number Major Minor RaidDevice State
    0         8      49        0 active sync  /dev/sdd1
    1         8      65        1 active sync  /dev/sde1
[root@localhost /]#
```

Снимок экрана 66 - Информация о RAID массиве

Изм	Лист	№ докум	Подп	Дата

## 9 ФИЛЬТРАЦИЯ СЕТЕВОГО ПОТОКА

Средства фильтрации сетевого потока предоставляют возможности фильтрации входящих и исходящих сетевых потоков на основе установленного набора правил с учетом атрибутов безопасности и используемых сетевых протоколов, а также управления правилами фильтрации сетевых потоков; регистрации и учета выполнения проверок при фильтрации сетевых потоков.

### 9.1 Утилита `firewall-cmd`

Утилита `firewall-cmd` позволяет настраивать работу брандмауэра, осуществляющего фильтрацию сетевых потоков при помощи определения так называемых зон, иными словами, наборов правил, которые управляют трафиком на основе уровня доверия к той или иной сети. Существуют следующие зоны:

`drop` - самый низкий уровень доверия сети. Весь входящий трафик сбрасывается без ответа, поддерживаются только исходящие соединения;

`block` - эта зона похожа на предыдущую, но при этом входящие запросы сбрасываются с сообщением `icmp-host-prohibited` или `icmp6-adm-prohibited`;

`public` - эта зона представляет публичную сеть, которой нельзя доверять, однако поддерживает входящие соединения в индивидуальном порядке;

`external` - зона внешних сетей. Поддерживает маскировку NAT, благодаря чему внутренняя сеть остается закрытой, но с возможностью получения доступа;

`internal` - обратная сторона зоны `external`. Компьютерам в этой зоне можно доверять. Доступны дополнительные сервисы;

`dmz` - используется для компьютеров, расположенных в DMZ (зонах изолированных компьютеров, которые не будут иметь доступа к остальной части сети), поддерживает только некоторые входящие соединения;

`work` - зона рабочей сети. Большинству машин в сети можно доверять, доступны дополнительные сервисы;

`home` - зона домашней сети. Окружению можно доверять, но поддерживаются только определённые пользователем входящие соединения;

`trusted` - всем машинам в сети можно доверять.

Изм	Лист	№ докум	Подп	Дата



Режимы работы утилиты и выполняемые функции задаются набором опций, в том числе:

- state. Вывести состояние брандмауэра;
- reload. Перезагрузить правила из постоянной конфигурации;
- complete-reload. Жёсткая перезагрузка правил с разрывом всех соединений;
- runtime-to-permanent. Перенести настройки runtime в постоянную конфигурацию;
- permanent. Использовать постоянную конфигурацию;
- get-default-zone. Отобразить зону, используемую по умолчанию;
- set-default-zone. Установить зону по умолчанию;
- get-active-zones. Отобразить активные зоны;
- get-zones. Отобразить все доступные зоны;
- get-services. Вывести predefined сервисы;
- list-all-zones. Вывести конфигурацию всех зон;
- new-zone. Создать новую зону;
- delete-zone. Удалить зону;
- list-all. Вывести всё, что добавлено, из выбранной зоны;
- list-services. Вывести все сервисы, добавленные к зоне;
- add-service. Добавить сервис к зоне;
- remove-service. Удалить сервис из зоны;
- list-ports. Отобразить порты, добавленные к зоне;
- add-port. Добавить порт к зоне;
- remove-port. Удалить порт из зоны;
- query-port. Показать, добавлен ли порт к зоне;
- list-protocols. Вывести протоколы, добавленные к зоне;
- add-protocol. Добавить протокол к зоне;
- remove-protocol. Удалить протокол из зоны;
- list-source-ports. Вывести порты источника, добавленные к зоне;
- add-source-port. Добавить порт-источник к зоне;
- remove-source-port. Удалить порт-источник из зоны;
- list-icmp-blocks. Вывести список блокировок icmp;
- add-icmp-block. Добавить блокировку icmp;
- remove-icmp-block. Удалить блокировку icmp;

Изм	Лист	№ докум	Подп	Дата

- add-forward-port. Добавить порт для перенаправления в NAT;
- remove-forward-port. Удалить порт для перенаправления в NAT;
- add-masquerade. Включить NAT;
- remove-masquerade. Удалить NAT.

Например, настройка правила блокировки адреса получателя может выглядеть следующим образом:

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -d 192.168.10.20 -j DROP
success
[root@localhost ~]# █
```

Снимок экрана 67 – Настройка правила блокировки адреса получателя

Настройка правила отбрасывания всех входящих соединений по протоколу IPv4 может выглядеть следующим образом:

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -j DROP
success
```

Снимок экрана 68 - Запрет входящих соединений по протоколу IPv4

Настройка правила отбрасывания всех исходящих пакетов UDP может выглядеть следующим образом:

```
[root@localhost ~]# firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p udp -j DROP
success
```

Снимок экрана 69 - Запрет использования сетевого протокола UDP

## 9.2 Конфигурационный файл /etc/firewalld/firewalld.conf

Конфигурационный файл /etc/firewalld/firewalld.conf содержит основные параметры конфигурации для брандмауэра firewalld (см. Снимки экрана 70 и 71), в том числе:

DefaultZone - устанавливает зону по умолчанию для соединений или интерфейсов;

MinimalMark - с этой опцией блок меток может быть зарезервирован для частного использования. Используются только отметки над этим значением. Значение по умолчанию равно 100;

Изм	Лист	№ докум	Подп	Дата

CleanupOnExit - если firewalld останавливается, он очищает все правила. Если для этого параметра установлено значение по или false, текущие правила останутся нетронутыми. Значением по умолчанию является yes или true;

Lockdown - если эта опция включена, изменения firewalld с интерфейсом D-Bus будут ограничены приложениями, которые перечислены в белом списке блокировки. Значением по умолчанию является по или false;

IPv6\_rpfilter - если эта опция включена, выполняется проверка фильтра обратного пути для пакета для IPv6. Если ответ на пакет будет отправлен через тот же интерфейс, на который поступил пакет, пакет совпадет и будет принят, в противном случае он будет отброшен. Для IPv4 rp\_filter управляется с помощью sysctl;

IndividualCalls - если этот параметр отключен, используются комбинированные вызовы restore, а не отдельные вызовы, чтобы применить изменения к брандмауэру. Использование отдельных вызовов увеличивает время, необходимое для применения изменений;

LogDeniel – добавление правил ведения журнала непосредственно перед отклонением и удалением правил в цепочках INPUT, FORWARD и OUTPUT для правил по умолчанию, а также окончательных правил отклонения и отбрасывания в зонах для настроенного типа пакета канального уровня. По умолчанию установлено off отключение ведения журнала.

AutomaticHelpers - для безопасного использования протокола IPv4 iptables и помощников по отслеживанию соединений этот параметр рекомендуется отключить. Возможные значения: *yes*, *no*, *system*, по умолчанию установлено *system*;

FirewallBackend - выбирает реализацию брандмауэра. Возможные значения: nftables (по умолчанию) или iptables. Это относится ко всем примитивам firewalld. Единственным исключением являются прямые и сквозные правила, которые всегда используют традиционные iptables, ip6tables и ebtables.

Изм	Лист	№ докум	Подп	Дата

```

# firewalld config file

# default zone
# The default zone used if an empty zone string is used.
# Default: public
DefaultZone=public

# Minimal mark
# Marks up to this minimum are free for use for example in the direct
# interface. If more free marks are needed, increase the minimum
# Default: 100
MinimalMark=100

# Clean up on exit
# If set to no or false the firewall configuration will not get cleaned up
# on exit or stop of firewalld
# Default: yes
CleanupOnExit=yes

# Lockdown
# If set to enabled, firewall changes with the D-Bus interface will be limited
# to applications that are listed in the lockdown whitelist.
# The lockdown whitelist file is lockdown-whitelist.xml
# Default: no
Lockdown=no

# IPv6_rpfilter
# Performs a reverse path filter test on a packet for IPv6. If a reply to the
# packet would be sent via the same interface that the packet arrived on, the
# packet will match and be accepted, otherwise dropped.
# The rp_filter for IPv4 is controlled using sysctl.
# Default: yes
IPv6_rpfilter=yes

```

Снимок экрана 70 - Конфигурационный файл /etc/firewalld/firewalld.conf (1)

```

# Clean up on exit
# If set to no or false the firewall configuration will not get cleaned up
# on exit or stop of firewalld
# Default: yes
CleanupOnExit=yes

# Lockdown
# If set to enabled, firewall changes with the D-Bus interface will be limited
# to applications that are listed in the lockdown whitelist.
# The lockdown whitelist file is lockdown-whitelist.xml
# Default: no
Lockdown=no

# IPv6_rpfilter
# Performs a reverse path filter test on a packet for IPv6. If a reply to the
# packet would be sent via the same interface that the packet arrived on, the
# packet will match and be accepted, otherwise dropped.
# The rp_filter for IPv4 is controlled using sysctl.
# Default: yes
IPv6_rpfilter=yes

# IndividualCalls
# Do not use combined -restore calls, but individual calls. This increases the
# time that is needed to apply changes and to start the daemon, but is good for
# debugging.
# Default: no
IndividualCalls=no

# LogDenied
# Add logging rules right before reject and drop rules in the INPUT, FORWARD
# and OUTPUT chains for the default rules and also final reject and drop rules
# in zones. Possible values are: all, unicast, broadcast, multicast and off.
# Default: off
LogDenied=off

```

Снимок экрана 71 - Конфигурационный файл /etc/firewalld/firewalld.conf (2)

Изм.	Лист	№ докум	Подп	Дата

## 10 МОНИТОРИНГ ФУНКЦИОНИРОВАНИЯ

Средства мониторинга функционирования предоставляют возможности слежения и сбора информации о выполнении пользовательских процессов и состоянии сетевого трафика.

### 10.1 Утилита logwatch

Утилита logwatch позволяет проводить анализ системных журналов по различным критериям с возможностью составления отчётов. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- detail level. Уровень детализации отчета. Может быть положительным целым числом или high, med, low, которые соответствуют целым числам 10, 5 и 0 соответственно;
- debug level. Уровень отладки. Может варьироваться от 0 до 100;
- logfile log-file-group. Обрабатывать только набор указанных файлов журналов;
- service service-name. Обрабатывать только указанную службу;
- print. Вывести результаты на экран;
- mailto address. Отправить результаты по указанному адресу электронной почты;
- save file-name. Сохранить вывод в указанный файл вместо отображения на экране или отправки по электронной почте;
- range range. Диапазон дат для обработки;
- archives. Искать в архивных журналах;
- logdir directory. Обрабатывать файлы журналов из указанного каталога, а не из каталога по умолчанию;
- hostname hostname. Обрабатывать файлы журналов только указанного хоста.

### 10.2 Утилита top

Утилита top предназначена для получения информации о выполняемых процессах. Режимы ее работы и реализуемые функции задаются набором опций, в том числе:

- u. Отображать только процессы с заданным идентификатором или именем пользователя;
- S. Отображать системные процессы;
- n. Изменить число отображаемых процессов на заданное число;
- i. Работа в интерактивном режиме, задается по умолчанию;

Изм	Лист	№ докум	Подп	Дата

- I. Не отображать бездействующие процессы, по умолчанию отображаются как активные, так и бездействующие процессы:

-c. Переключение отображения командных строк на отображение имен программ и наоборот;

-s. Задаёт временной интервал задержки между обновлениями экрана, по умолчанию 5 секунд;

-b. Работа в пакетном режиме, может использоваться для отправки результатов в другие программы или в файл;

-o. Задаёт имя поля, по которому будет осуществляться сортировка, используется в основном для пакетного режима;

-w. Задаёт форматирование вывода по ширине, количество строк считается неограниченным;

-v. Показать версию утилиты и выйти;

-h. Показать справку и выйти.

Например, определение списка работающих в системе процессов может выглядеть следующим образом:

```
top - 10:17:12 up 1 day, 1:14, 10 users, load average: 0,31, 0,23, 0,30
Tasks: 325 total, 1 running, 324 sleeping, 0 stopped, 0 zombie
%Cpu(s): 12,8 us, 2,3 sy, 0,0 ni, 84,9 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem : 1016800 total, 60492 free, 802564 used, 153744 buff/cache
KiB Swap: 1048572 total, 292260 free, 756312 used. 35164 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
19450	gdm	20	0	1387940	48356	6424	S	3,6	4,8	9:19.75	gnome-shell
17444	gdm	20	0	1384972	47972	6260	S	3,0	4,7	9:41.23	gnome-shell
25612	gdm	20	0	1383696	65536	9440	S	2,6	6,4	0:45.14	gnome-shell
21832	gdm	20	0	1383364	41248	6392	S	2,3	4,1	5:51.40	gnome-shell
16358	user3	20	0	1502636	159852	13132	S	1,0	15,7	2:16.46	gnome-shell
16958	user3	20	0	560316	11908	4328	S	0,7	1,2	0:09.36	gnome-terminal -
19420	gdm	20	0	34816	824	568	S	0,3	0,1	0:25.83	dbus-daemon
<b>26473</b>	<b>root</b>	<b>20</b>	<b>0</b>	<b>157840</b>	<b>2400</b>	<b>1524</b>	<b>R</b>	<b>0,3</b>	<b>0,2</b>	<b>0:00.05</b>	<b>top</b>
1	root	20	0	194252	3160	1268	S	0,0	0,3	0:03.95	systemd
2	root	20	0	0	0	0	S	0,0	0,0	0:00.01	kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:00.92	ksoftirqd/0
7	root	rt	0	0	0	0	S	0,0	0,0	0:00.00	migration/0
8	root	20	0	0	0	0	S	0,0	0,0	0:00.00	rcu_bh
9	root	20	0	0	0	0	S	0,0	0,0	0:07.33	rcu_sched
10	root	rt	0	0	0	0	S	0,0	0,0	0:01.05	watchdog/0
12	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	khelper
13	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kdevtmpfs
14	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	netns
15	root	20	0	0	0	0	S	0,0	0,0	0:00.03	khungtaskd
16	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	writeback
17	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kintegrityd
18	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	bioaset

Снимок экрана 72 - Определение списка работающих процессов

Изм	Лист	№ докум	Подп	Дата

### 10.3 Утилита ps

Утилита ps используется для получения информации о состоянии текущих процессов. Режимы ее работы задаются набором опций, в том числе:

- u. Выводить информацию только о процессах с заданными списком эффективными идентификационными номерами или идентификаторами пользователей;
- Y. Выводить информацию только о процессах с заданными списком реальными идентификационными номерами или идентификаторами пользователей;
- g. Выводить информацию только о процессах с заданными списком идентификационными номерами групп;
- G. Выводить информацию только о процессах с заданными списком реальными идентификационными номерами групп;
- a. Выводить информацию о состоянии наиболее часто запрашиваемых процессов;
- e. Выводить информацию для всех процессов;
- d. Выводить информацию о всех процессах, кроме лидеров сеансов;
- r. Выводить информацию только для запущенных процессов;
- G. Выводить информацию о процессах, чьи реальные номера групп указаны в заданном списке;
- o. Выводить информацию в заданном формате.

### 10.4 Утилита tcpdump

Утилита tcpdump предназначена для мониторинга и анализа сетевого трафика. Состоит из двух частей: части захвата пакетов с копированием их в так называемый буфер и части отображения захваченных пакетов из буфера. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- i. Задаёт интерфейс, с которого необходимо анализировать трафик;
- u. Устанавливает тип канала передачи данных для использования во время захвата пакетов;
- e. Включает вывод данных канального уровня;
- v. Вывод дополнительной информации;
- w. Задаёт имя файла, в котором будет сохраняться собранная информация;
- r. Захватывать только трафик, предназначенный данному узлу;

Изм	Лист	№ докум	Подп	Дата

- q. Переводит работу в "бесшумный режим", в котором пакет анализируется на транспортном уровне, а не на сетевом;
- t. Отключает вывод меток времени;
- A. Вывод пакетов в формате ASCII без заголовков канального уровня;
- B. Установить размер буфера захвата;
- D. Вывести список доступных сетевых интерфейсов, на которых может осуществляться захват пакетов.

### 10.5 Утилита as

Утилита as предназначена для получения информации о сеансах пользователей. Режимы ее работы и выполняемые функции задаются набором опций, в том числе:

- p. Выводить итоговое время сеансов каждого пользователя;
- d. Кроме общих итогов, выводить итоги за каждый день;
- a. При выводе ежедневных итогов не пропускать дни, когда входов в систему не было;
- y. Выводить год при отображении даты;
- z. Если итоговое значение равно нулю, то выводить его. По умолчанию не выводится;
- v. Вывести номер версии;
- h. Вывести краткую справку.

### 10.6 Утилита lastcomm

Утилита lastcomm позволяет получить информацию о последних выполненных командах. Режимы ее работы задаются набором опций, в том числе:

- E. Выводить время начала процесса выполнения команды;
- S. Выводить время завершения процесса выполнения команды;
- c. Выводить количество использованного процессорного времени;
- e. Выводить количество использованного прошедшего времени;
- s. Выводить количество использованного системного времени;
- u. Выводить количество использованного пользовательского времени;
- f. Использовать заданный файл в качестве источника учетных данных, он может быть либо стандартным, либо расширенным файлом учета процесса;
- x. Использовать текущий расширенный файл учета процесса.

Изм	Лист	№ докум	Подп	Дата



